

Communication Modules

EtherNet/IP Communication Module

2789-9023



© 2023 WAGO GmbH & Co. KG
All rights reserved.

WAGO GmbH & Co. KG

Hansastraße 27
D - 32423 Minden

Phone: +49 571/887 – 0
Fax: +49 571/887 – 844169
E-Mail: ✉ info@wago.com
Internet: 🌐 www.wago.com

Technical Support

Phone: +49 571/887 – 44555
Fax: +49 571/887 – 844555
E-Mail: ✉ support@wago.com

Every conceivable measure has been taken to ensure the accuracy and completeness of this documentation. However, as errors can never be fully excluded, we always appreciate any information or suggestions for improving the documentation.

E-Mail: ✉ documentation@wago.com

We wish to point out that the software and hardware terms as well as the trademarks of companies used and/or mentioned in the present manual are generally protected by trademark or patent.

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Table of Contents

Provisions	6
1.1 Intended Use	6
1.2 Typographical Conventions	7
1.3 Legal Information	9
Safety	10
2.1 General Safety Rules	10
2.2 Electrical Safety	10
2.3 Mechanical Safety	10
2.4 Thermal Safety	11
2.5 Indirect Safety	11
Properties	12
3.1 Overview	12
3.2 View	12
3.3 Type label	13
3.4 Product-Specific Information	14
3.5 Connections	15
3.5.1 RJ-45 Interfaces	15
3.6 Indicators	16
3.7 Control Elements	16
3.8 Technical data	16
3.8.1 Product	16
3.8.2 Power Loss	17
3.8.3 Communication	17
3.8.4 Environmental Conditions	17
3.9 Guidelines, approvals and standards	17
3.9.1 Guidelines	17
3.9.2 Approvals	18
3.9.3 Standards	19
Fieldbus Description	20
4.1 Technology	20
4.1.1 EtherNet/IP Overview	20
4.1.2 EDS File	20
4.2 Overview of the Objects	21
4.2.1 Identity Object	22
4.2.1.1 Instances	22
4.2.1.2 General Services	24
4.2.2 Assembly Object	24
4.2.2.1 Instances	25
4.2.2.2 General Services	26
4.2.3 Connection Object	26

4.2.4	Connection Manager Object.....	26
4.2.5	TCP/IP Interface Object	26
4.2.5.1	Instances	26
4.2.5.2	General Services.....	28
4.2.6	Ethernet Link Object.....	28
4.2.6.1	Instances.....	28
4.2.6.2	General Services.....	31
4.2.7	Device Parameter Object	31
4.2.7.1	General Device Parameters of Lower-Level Devices.....	31
4.2.7.2	Device Parameters of the WAGO Pro 2 Power Supply.....	33
4.2.7.3	General Services.....	35
4.2.8	Module Parameter Object	36
4.2.9	Measurement Data Object	38
4.2.9.1	Events and Measured Values	38
4.2.9.2	General Services.....	40
4.3	MQTT	41
4.3.1	Connection Status	41
4.3.2	Data Exchange.....	41
4.3.3	Application Examples	44
	Transport and Storage	45
	Installation and Removal	46
	Commissioning.....	48
7.1	Setting an IP address	48
7.1.1	Assigning an IP Address Using DHCP	48
7.1.2	Setting a Static IP Address.....	49
	Operation.....	51
8.1	Operating via Reset Button	51
	Configuration	52
9.1	Configuring with WBM	52
9.1.1	Logging In.....	52
9.1.2	Menu Page	52
9.1.3	Module Settings.....	53
9.1.4	Module Information.....	57
9.1.5	Device Settings	58
9.1.6	Device Information	62
9.1.7	Device Measurement	62
9.1.8	Configuration of Communication with Broker	63
	Decommissioning.....	66
10.1	Disposal and Recycling	66
	Appendix	67
11.1	User Certificates	67
11.1.1	Creating and Replacing Certificates	68
11.1.2	Creating a Template for Certificates.....	68
11.1.3	Creating the Root CA Certificate	71
11.1.4	Creating the Device Certificate.....	75

- 11.1.5 Exporting WBM Certificates..... 80
- 11.1.6 Exporting MQTT Certificates 82
- 11.1.7 Installing WBM Certificates on the Client and Product..... 85
- 11.1.8 Installing MQTT Certificates on the Broker and Product..... 86
- 11.2 Accessories 87
- 11.3 Protected Rights 87

Provisions

This document applies to the following product:

2789-9023 (EtherNet/IP Communication Module)

Product detail page	www.wago.com/2789-9023
---------------------	--

The product must only be installed and operated in accordance with the operating instructions. Knowledge of the operating instructions is required for proper use. You can find all documents and information on the detailed product page.

Additional document

-  **Product Manual** of the Pro 2 Power Supply used

1.1 Intended Use

The 2789 Series EtherNet/IP Communication Module is used for communication with a EtherNet/IP fieldbus environment and is plugged into a subordinate WAGO Power Supply Pro 2.

The product is an open equipment and is designed for installation in an additional enclosure.

- This product is intended for installation in automation technology systems.
- The product is designed for use in dry indoor rooms.
- Operation of the products in industrial area is permitted.
- The product meets the EMC requirements for the residential, office and commercial area as well as small business, if the product used complies with the required emissions of interference (emission limits).
- Operation of the product in other application areas is only permitted when corresponding approvals and labeling are present.

Improper Use

Improper use of the product is not permitted. Improper use occurs especially in the following cases:

- Non-observance of the intended use
- Use without protective measures in an environment in which moisture, salt water, salt spray mist, dust, corrosive fumes, gases, direct sunlight or ionizing radiation can occur
- Use of the product in areas with special risk that require continuous fault-free operation and in which failure of or operation of the product can result in an imminent risk to life, limb or health or cause serious damage to property or the environment (such as the operation of nuclear power plants, weapons systems, aircraft and motor vehicles)

Warranty and Liability

The terms set forth in the General Business and Contract Conditions for Delivery and Service of WAGO GmbH & Co. KG and the terms for software products and products with integrated software stated in the WAGO Software License Contract – both available at

www.wago.com – shall apply. In particular, the warranty is void if:

- The product is improperly used.

- The deficiency (hardware and software configurations) is due to special instructions.
- Modifications to the hardware or software have been made by the user or third parties that are not described in this documentation and that has contributed to the fault.

Individual agreements always have priority.

Obligations of Installers/Operators

Installers and operators bear responsibility for the safety of an installation or a system assembled with the product. The installer/operator is responsible for the proper installation and safety of the system. All laws, standards, guidelines, local regulations and accepted technological standards and practices applicable at the time of installation, as well as the products' operating instructions, must be followed. In addition, the installment requirements for approval must be met. In the event of non-compliance, operation of product within the scope of the approval is not permitted.

In addition, the installer/operator is responsible for the deployment of suitable personnel.

1.2 Typographical Conventions





Number Notation

100	Decimals: Normal notation
0x64	Hexadecimals: C-notation
'100'	Binary: In single quotation marks
'0110.0100'	Nibbles separated by a period

Text Formatting

<i>italic</i>	Names of paths or files
bold	Menu items, entry or selection fields, emphasis
Code	Sections of program code
>	Selection of a menu point from a menu
"Value"	Value entries
[F5]	Identification of buttons or keys

Cross References / Links

	Cross references/links to a topic in a document
	Cross references / links to a separate document
	Cross references / links to a website
	Cross references / links to an email address

Sequence of Action

- ✓ This symbol identifies a precondition.
- 1. Action step
- 2. Action step
- ⇒ This symbol identifies an intermediate result.

⇒ This symbol identifies the result of an action.

- Individual action step

Lists

- Lists, first level
 - Lists, second level

Figures

Figures in this documentation are for better understanding and may differ from the actual product design.

Warning Notices

DANGER

Type and source of hazard

Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.

- Action step to reduce risk

WARNING

Type and source of hazard

Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

- Action step to reduce risk

CAUTION

Type and source of hazard

Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

- Action step to reduce risk

NOTICE

Type and source of malfunction (property damage only)

Indicates a potentially hazardous situation which, if not avoided, may result in damage to property.

- Action step to reduce risk

Information Notices

Note

Information


Indicates information, clarifications, recommendations, referrals, etc.

1.3 Legal Information

Intellectual property

The intellectual property of this document belongs to WAGO GmbH & Co. KG. The reproduction and distribution of its content (in whole or in part) is prohibited, unless otherwise provided by statutory provisions, written agreements or this document. In case of doubt, the written consent of WAGO GmbH & Co. KG must be obtained in advance.


Third-party products are always mentioned without any reference to patent rights. WAGO GmbH & Co. KG, or the manufacturer of third-party products, retains all rights regarding patent, utility model or design registration.

Third-party trademarks are referred to in the product documentation. The “®” and “™” symbols are omitted hereinafter. The trademarks are listed in the Appendix:  **Protected Rights [▶ 87]**.

Subject to Change

The instructions, guidelines, standards, etc., in this manual correspond to state of the art at the time the documentation was created and are not subject to updating service. The installer and operator bear sole responsibility to ensure they are complied with in their currently applicable form. WAGO GmbH & Co. KG retains the right to carry out technical changes and improvements of the products and the data, specifications and illustrations of this manual. All claims for change or improvement of products that have already been delivered – excepting change or improvement performed under guarantee agreement – are excluded.

Licenses

The products may contain open-source software. The requisite license information is saved in the products. This information is also available under:  www.wago.com.

Safety

2.1 General Safety Rules

- This documentation is part of the product. Therefore, retain the documentation during the entire service life of the product. Pass on the documentation to any subsequent user of the product. In addition, ensure that any supplement to this documentation is included, if necessary.
- The product must only be installed and put into operation by qualified electrical specialists per EN 50110-1/-2 and IEC 60364.
- Comply with the laws, standards, guidelines, local regulations and accepted technology standards and practices applicable at the time of installation.

2.2 Electrical Safety

- Make sure the product does not carry any voltage before starting work.

Grounding/Protection/Fuses

- When handling the product, please ensure that environmental factors (personnel, work space and packaging) are properly equalized. Do not touch any conducting parts.

Cables

- Use shielded cables with copper braiding or tinned copper braiding. This reduces electromagnetic interference and increases signal quality. Measurement errors, data transmission errors and interference due to excessive voltage can be prevented.
- Maintain spacing between control, signal and data lines and the power supply lines.
- Observe permissible temperature range of connecting cables.
- Use appropriate strain relief.

2.3 Mechanical Safety

- As the installer of the system, you are responsible for ensuring the necessary touch-proof protection. Follow the installation guidelines for the specific application.
- Before startup, please check the product for any damage that may have occurred during shipping. Do not put the product into operation in the event of mechanical damage.
- Do not open the product housing.
- The product is an open-type device and is designed for installation in an additional enclosure, which supplies the following safety aspects:
 - Restrict access to authorized personnel and may only be opened with tools.
 - Ensure the required pollution degree in the vicinity of the system.
 - Offer adequate protection against direct or indirect contact.
 - Offer adequate protection against UV irradiation.
 - Prevent fire from spreading outside of the enclosure.
 - Guarantee mechanical stability.

2.4 Thermal Safety

- The surface of the housing heats up during operation. Under special conditions (e.g., in the event of a fault or increased surrounding air temperature), touching the product may cause burns. Allow the product to cool down before touching it.
- The temperature inside the additional enclosure must not exceed the surrounding air temperature permitted for the mounted product.
- Cooling of the product must not be impaired. Ensure air can flow freely and that the minimum clearances from adjacent products/areas are maintained.

2.5 Indirect Safety

- Only use a dry or cloth or a clothed dampened with water to clean the product. Do not use cleaning agents, e.g., abrasive cleaners, alcohols or acetone.
- Clean tools and materials are imperative for handling the product.
- The product contains no parts that can be serviced by the user. Always have all service, maintenance and repair work performed by specialists authorized by WAGO.
- Replace any defective or damaged devices.

Properties

3.1 Overview

This product supports ETHERNET-based communication with a lower-level device (such as a WAGO Power Supply Pro 2 with firmware version 01.04.xx or higher). It functions as a gateway.

The following protocols are supported:

- EtherNet/IP (Industrial Protocol)
- BootP (pending)
- DHCP
- SNTP
- HTTP(S)
- MQTT

The integrated switch with two external RJ45 ports makes it possible to set up a line topology without additional infrastructure elements such as switches or hubs.

3.2 View

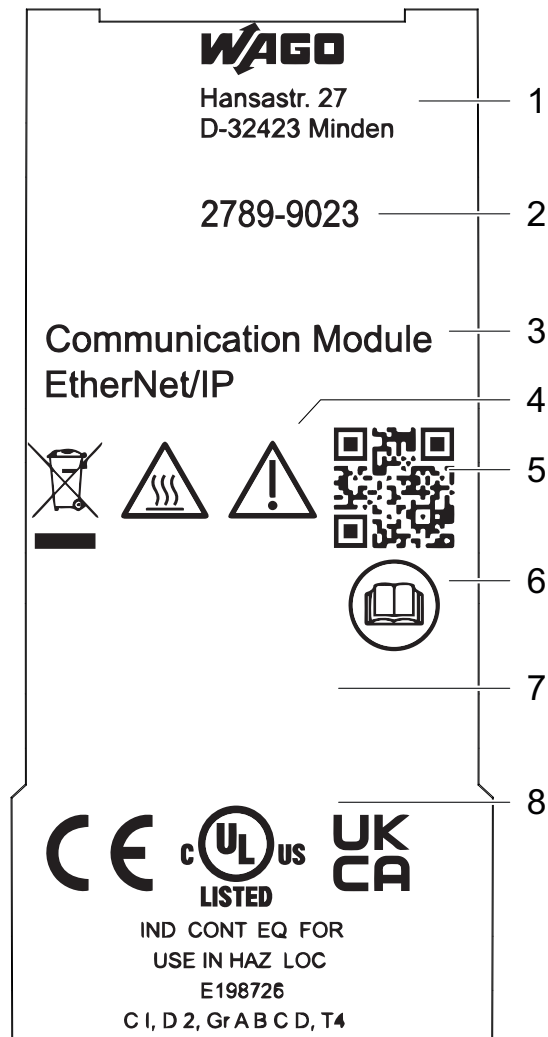


Figure 1: View

Position	Comment	Details
a	Locking tab	–
b	Ventilation openings	–
c	Optical status indication	Indicators [▶ 16]
d	Reset button	Operating via Reset Button [▶ 51]
e	Communication interface	–
f	Type label	Type label [▶ 13]
g	Marker carrier	Accessories [▶ 87]
h	ETHERNET port 1 (X5); ETHERNET port 2 (X6)	–

3.3 Type label

The product's type plate contains the following information:



Position	Comment	Details
1	Company logo and address	–
2	Item number	–
3	Product name	–
4	Warning notice symbols	Safety [▶ 10]
5	QR link with link to website	–
6	Reference to product documentation	–
7	Product-specific information	Product-Specific Information [▶ 14]
8	Box for approvals	Approvals [▶ 18]

3.4 Product-Specific Information

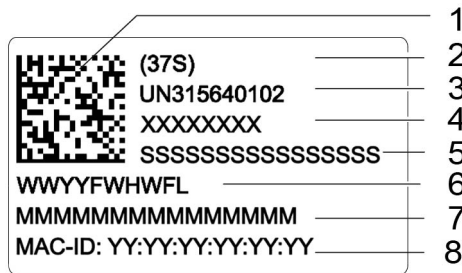


Figure 2: Product-Specific Information

Position	Comment	Details
1	2D data matrix code	Contains the information for positions 2 ... 5
2	Key number	Fixed information (37S)
3	ID number per D-U-N-S®	Fixed information (WAGO Minden)
4	WAGO item number or internal SAP number	Product-specific
5	Consecutive number	Product-specific
6	Production date and revision	<ul style="list-style-type: none"> Production date Revision index (FW HW FL)
7	Internal manufacturer product number	Product-specific
8	Media Access Control Identifier	Product-specific

Table 1: Revision index structure

Software index	Hardware index	Boot loader index
FW	HW	FL

3.5 Connections

3.5.1 RJ-45 Interfaces

The connection to ETHERNET-based fieldbuses is established via two RJ45 connectors (see figure “RJ45 Interface, X5/X6”), also called “Western plugs,” which are connected to the fieldbus controller via an integrated switch.

The integrated switch works in store-and-forward mode and supports 10/100 Mbit/s transmission speeds, as well as full and half-duplex transmission modes, for each port.

The RJ45 sockets are wired in accordance with the specifications for 100BASE-TX.

The ETHERNET standard stipulates a twisted pair cable of at least Category 5e as a connecting cable. S/UTP (Screened Unshielded Twisted Pair) and STP (Shielded Twisted Pair) type cables with a maximum segment length of 100 m can be used.

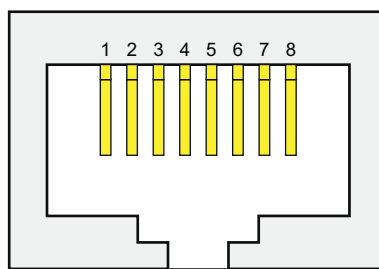


Figure 3: RJ45 Interface, X5/X6

Pin	Description
1	TD +
2	TD -
3	RD +
4	-
5	-
6	RD -
7	-
8	-

The pin assignments for RJ45 connectors are specified in the EIA/TIA 568 standard. TD: Transmit Data. RD: Receive Data.

3.6 Indicators

The product has a visual status indicator. This indicator consists of six LEDs.













- ERR 
- COM OK 
- LNK/ACT1 
- SPEED1 
- LNK/ACT2 
- SPEED2 


Figure 4: Visual Status Indicator

Table 2: Operating Status Indication

Indicator	LED Description	State	Description	
ERR		Error	Off	Ready for operation; no error
			On	General error/system error
			Flashing (8 Hz)	EtherNet/IP connection error
			Flashing (16 Hz)	Communication module is resetting to factory defaults
COM OK		Device status	Off	No connection to lower-level device
			On	Initialization
			Flashing (2 Hz)	Communication active
			Flashing (16 Hz)	IP address is being assigned via DHCP
LNK/ACT1		Port 1: connection/activity	Off	No connection present
			On	Connection present, but no activity
			Flashing	Connection and activity present
SPEED1		Port 1: speed	Off	Connection rate: 10 Mbit/s
			On	Connection rate: 100 Mbit/s
LNK/ACT2		Port 2: connection/activity	Off	No connection present
			On	Connection present, but no activity
			Flashing	Connection and activity present
SPEED2		Port 2: speed	Off	Connection rate: 10 Mbit/s
			On	Connection rate: 100 Mbit/s

3.7 Control Elements

A reset button is located on the front of the product. This button can be used to reset the product.

See  [Operating via Reset Button \[▶ 51\]](#) for a detailed description of how you can use the reset button to make settings.

3.8 Technical data

3.8.1 Product

Table 3: Technical Data – Product

Property	Value
Width	35 mm
Height	80 mm

Property	Value
Depth	22 mm
Weight	45 g
Degree of protection	IP20

3.8.2 Power Loss

Table 4: Technical Data – Power Loss

Property	Value
Power loss (max.)	1.1 W

3.8.3 Communication

Table 5: Technical Data – Communication

Property	Value
Communication	Ethernet/IP
Interface	RJ-45 interface
Cable length	≤ 100 m
Transmission medium	Twisted pair, shielded
Transmission rate	100 MBd (ETHERNET: 10/100 Mbit/s)
ETHERNET protocols	HTTP(S), BootP *, DHCP, SNTP
Specifications of the conductors used	≥ +75 °C (ambient air temperature: ≤ +60 °C)

^{*)} Pending

3.8.4 Environmental Conditions

Table 6: Technical Data – Environmental Conditions

Property	Value
Test voltage (fieldbus)	0.775 kVAC, 50 Hz, 1 min.
Type of insulation	Functional insulation
Ambient temperature, operation ¹⁾	-40 ... +55 °C
Ambient temperature, storage	-40 ... +85 °C
Relative humidity	5 ... 95 % (no condensation)
Elevation above sea level, max.	5000 m
Pollution degree according to IEC/EN 60664-1	2
Protection class	III
Protection type ²⁾	IP20

¹⁾ When the EtherNet/IP™ communication module is used in combination with a WAGO Power Supply Pro 2 approved for a maximum ambient temperature of +70 °C, a maximum ambient temperature of +55 °C must not be exceeded during operation.

²⁾ The lower-level WAGO Power Supply Pro 2

3.9 Guidelines, approvals and standards

3.9.1 Guidelines




An EU “Declaration of Conformity” and CE marking exist for the product.

For additional information, visit www.wago.com.

3.9.2 Approvals

The following approvals have been granted for the product:

Table 7: Approvals

Logo	Certification Body	Standard
	Underwriters Laboratories Inc. (Ordinary Locations)	UL 61010-1
	Underwriters Laboratories Inc. (Ordinary Locations)	UL 61010-2-201
	Underwriters Laboratories Inc. (Hazardous Locations)	UL 121201

Note

More information on approvals

You can find detailed information on the approvals online at:

 www.wago.com/<item number>

3.9.3 Standards

Table 8: Mechanical and Climatic Environmental Conditions

Standard	Test Value
Mechanical Environmental Conditions	
EN 60068-2-6	f = 5 ... 150 Hz: 1g, 3.5 m
IEC 60068-2-27, Shock	15g, 11 ms, 6 shocks per axis and direction, half-sine
EN 61131-2, Section 4.3	Freefall ≤ 300 mm (packaged in the product packaging)
Climatic Environmental Conditions	
EN 60870-2-2	3K3 (except for low air pressure)

Table 9: EMV – Immunity to Interference

Standard	Title
EN 61000-6-2	Part 6-2: Generic standards – Immunity for industrial environments*
EN 61000-4-2	Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test
EN 61000-4-3	Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test
EN 61000-4-4	Part 4-4: Testing and measurement techniques – Electrical fast transient/ burst immunity test
EN 61000-4-5	Part 4-5: Testing and measurement techniques – Surge immunity test
EN 61000-4-6	Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, induced by radio-frequency fields

* Interference may lead to performance deviations.

Table 10: EMC – Emission of Interference

Standard	Title
EN 61000-6-3	Part 6-3: Generic standards – Emission standard for residential, commercial and light-industrial environments

Fieldbus Description

4.1 Technology

4.1.1 EtherNet/IP Overview

EtherNet/IP is based on the TCP/IP protocol family and handles the lower four layers of the OSI layer model in unmodified form so that all standard ETHERNET communication modules, such as PC interface cards, cables, connectors, hubs, switches etc., can be used with EtherNet/IP in the same way. The “Encapsulation Protocol,” with which the “Common Industrial Protocol” (CIP) is superimposed on TCP/IP and UDP/IP, is located above the transport layer.

CIP is already used as a major network-independent standard for ControlNet and DeviceNet. Therefore, transferring an application to one of these systems is very feasible and easy. The data exchange is based on an object model.

ControlNet, DeviceNet and EtherNet/IP all have the same application protocol and can therefore use common device profiles and object libraries. These objects enable plug-and-play interoperability between complex devices from different manufacturers.

4.1.2 EDS File

The “Electronic Data Sheet” (EDS) file contains the product characteristics and information regarding its communication capabilities. The EDS file required for operation is imported/installed by the corresponding configuration software. Observe the installation notes in the documentation of the EDS file for the configuration software you are using.

Note

Downloading the EDS file

You can download the EDS file from the download area of the WAGO website:

 www.wago.com/2789-9023.

4.2 Overview of the Objects

The CIP objects are specified in the CIP specification of ODVA. WAGO uses classes 0x01, 0x04, 0x05, 0xF4, 0xF5 and 0xF6.

In addition, three specific WAGO objects are available.

All listed CIP common objects and WAGO-specific objects are described below.

Table 11: Overview of CIP Common Classes

Class	Object Name
0x01	Identity
0x04	Assembly
0x05	Connection
0x06	Connection Manager
0xF5	TCP/IP Interface Object
0xF6	Ethernet Link Object

Table 12: Overview of WAGO-Specific Classes

Class	Object Name
0x78	Module Parameter
0x82	Device Parameter
0x8C	Measurement Data

Table 13: Explanation of the Table Headings in the Object Descriptions

Column Header	Description
Attribute ID	Integer value assigned to the respective attribute
Access	<p>Set: The attribute can be accessed using the Set_Attribute service (writing/modifying the attribute value). If an attribute supports the Set_Attribute service, it can also be addressed with the Get_Attribute service.</p> <p>Get: The attribute can be accessed through the Get_Attribute service (reading the attribute value).</p> <p>Get_Attribute_All: returns the content of all attributes</p> <p>Set_Attribute_Single: modifies an attribute value</p> <p>Reset: performs a restart 0: Restart 1: restart and restore factory settings</p>
Name	Attribute identifier
Data type	Identifier for the CIP data type of the attribute
Description	Brief description of the attribute
Factory setting	Value of the factory setting

Table 14: Data Types Used

Data type	Description
UINT8	Unsigned 8 bit integer
UINT16	Unsigned 16 bit integer
UINT32	Unsigned 32 bit integer
CHAR[n]	A string of <i>n</i> characters
Padded EPATH ¹⁾	Byte array as application path

Data type	Description
STRUCT of:	Combines multiple parameters into one structure
1) Electronic Key Segment	

4.2.1 Identity Object

The Identity object (Class 0x01) provides general information about the product that can be used to clearly identify it.

4.2.1.1 Instances

Table 15: Identity Object – Instance 0

Attribute ID	Access	Name	Data type	Description	Factory setting
1	Get	Revision	UINT16	Version of this object	2
2	Get	Max Instance	UINT16	Maximum number of instances	1
3	Get	Number of Instances	UINT16	Number of instances	1

Table 16: Identity Object – Instance 1

Attribute ID	Access	Name	Data type	Description	Factory setting	
1	Get	Vendor ID	UINT16	Manufacturer identifier	40	
2	Get	Device Type	UINT16	General type designation of the product	12	
3	Get	Product Code	UINT16	Product identifier	32769	
4	Get	Revision	STRUCT of:	Version of the Identity object		
		Major Revision	UINT16			
		Minor Revision	UINT16			
5	Get	Status	UINT16	Current status of the product	Bit 0	Assignment to a master
					Bit 1 = 0	Reserved
					Bit 2 = 0	The product is not configured
					Bit 2 = 1	The product is configured
					Bit 3 = 0	Reserved
					Bits 4 ... 7	Extended device status
					Bits 4 ... 7 = 0010	At least one faulty I/O connection has been established
					Bits 4 ... 7 = 0011	No I/O connection established
					Bits 8 ... 11	Reserved
					Bits 12 ... 15 = 0	Reserved
6	Get	Serial Number	UINT32	Serial number	Serial number of the product	

Attribute ID	Access	Name	Data type	Description	Factory setting
7	Get	Product Name	CHAR[]	Product name	WAGO Communication Module

4.2.1.2 General Services

This object supports the following common services.

Table 17: Common Services

Service Code	Service Available		Service Name	Description
	Class	Instance		
0x01	Yes	Yes	Get_Attribute_All	Returns the content of all attributes
0x05	No	Yes	Reset	Performs a restart 0: restart 1: restart and restore factory settings
0x0E	No	Yes	Get_Attribute_Single	Returns the content of the respective attribute

4.2.2 Assembly Object

The Assembly object (class 0x04) binds attributes of different objects so that data can be sent to or received from each object via a connection. For example, these might include input and output data, status and control information or diagnostic information. WAGO uses the manufacturer-specific instances to provide these objects for you in various arrangements. This gives you an efficient way to exchange process data. The following is a description of the individual static Assembly instances with their contents and arrangements.

4.2.2.1 Instances

Assembly instance 101 (attribute ID 3) contains the process input data.

Table 18: Assembly Object – Instance 101, Attribute ID 3

No.	Access	Name	Data type	Description	
1	Get	EtherNet/IP module status	UINT16	Bit 0	Communication with lower-level device OK
				Bits 1 ... 15	Reserved
2	Get	Output voltage (mV)	UINT16		
3	Get	Output current (mA)	UINT16		
4	Get	Status	UINT16	Bit 0	DC status OK
				Bit 1	Overheating status
				Bit 2	No output voltage
				Bit 3	Output, short circuit
				Bit 4	Digital input status
				Bits 5 ... 15	Reserved
5	Get	Warnings	UINT16	Bit 0	Output, undervoltage
				Bit 1	Output, overvoltage
				Bit 2	Overload
				Bit 3	Adjustable output current limit exceeded
				Bit 4	Adjustable operating hours limit exceeded
				Bit 5	TopBoost supplied
				Bit 6	PowerBoost supplied
				Bit 7	High device temperature
				Bits 8 ... 15	Reserved
6	Get	Error	UINT16	Bit 0	Overheating, device switched off
				Bit 1	No output voltage
				Bit 2	Output short circuit
				Bit 3	Electronic circuit breaker tripped

Assembly Instance 102 contains process output data.

Table 19: Assembly Object – Instance 102

Attribute ID	Access	Name	Data type	Description	
3	Get/Set	Control word	UINT16	Bit 0	Device standby (not supported)
				Bit 1	Digital output on
				Bits 2 ... 15	Reserved

The software inspects the writing of attribute 3 of Assembly instance 102. If the limit value has been exceeded, it is identified and, if necessary, corrected. However, a write request is not rejected.

Assembly instance 103 is provided as a configuration object for implicit communication. The object is not used and returns no data when read out.

4.2.2.2 General Services

This object supports the following common services.

Table 20: Common Services

Service Code	Service Available		Service Name	Description
	Class	Instance		
0x0E	Yes	Yes	Get_Attribute_All	Returns the content of all attributes
0x10	No	Yes	Get_Attribute_Single	Returns the content of the respective attribute

4.2.3 Connection Object

Because the connections are established and terminated via the Connection Manager, the class and instance attributes of this object (class 0x05) are not visible.

4.2.4 Connection Manager Object

The Connection Manager object (Class 0x06) provides the internal resources required for the input and output data and explicit messages. In addition, this object is responsible for managing these resources. For each connection (input and output data or explicit data), another instance of the Connection class is created. The connection parameters are extracted from the “Forward Open” service, which is responsible for establishing a connection.

The following services are supported for the first instance: Forward_Open, Unconnected_Send and Forward_Close.

No class and instance attributes are visible.

4.2.5 TCP/IP Interface Object

The TCP/IP Interface object (Class 0xF5) provides for the configuration of the TCP/IP network interface. Examples of configurable objects include the IP address, the network mask and the gateway address of the product.

The underlying physical communication interface linked to the TCP/IP interface object can be any interface supported by the TCP/IP protocol. Examples of components that can be linked to a TCP/IP interface object include the following: an Ethernet 802.3 interface, an ATM (Asynchronous Transfer Mode) interface or a serial interface for protocols such as PPP (Point-to-Point Protocol). The TCP/IP Interface object provides an attribute, which is identified by the link-specific object for the connected physical communication interface. The link-specific object should typically provide link-specific counters, as well as any link-specific configuration attributes.

Each device must support exactly one instance of the TCP/IP Interface object for each TCP/IP-compatible communication interface.

4.2.5.1 Instances

Table 21: TCP/IP Interface Object – Instance 0

Attribute ID	Access	Name	Data type	Description	Factory setting
1	Get	Revision	UINT16	Version of this object	4
2	Get	Max Instance	UINT16	Maximum number of instances	1

Attribute ID	Access	Name	Data type	Description	Factory setting
3	Get	Number of Instances	UINT16	Number of connections currently instantiated	1

Table 22: TCP/IP Interface Object – Instance 1

Attribute ID	Access	Name	Data type	Description	Factory setting
1	Get	Status	UINT32	Interface status	
2	Get	Configuration Capability	UINT32	Interface flags for possible configuration types	0x00000054
3	Get/Set	Configuration Control	UINT32	Determines how the product coupler arrives at its TCP/IP configuration after the first restart	0x00000002
4	Get	Physical Link Object	STRUCT of:		
		Path Size	UINT16	Number of 16 bit words in the subsequent path	0x0002
		Path	Padded EPATH	Logical path that points to the physical link object	0x20, 0xF6, 0x24, 0x01 (corresponds to the Ethernet Link Object)
5	Get/Set	Interface Configuration	STRUCT of:		
		IP Address	UINT32	IP address	192.168.1.17
		Network Mask	UINT32	Network mask	255.255.255.0
		Gateway Address	UINT32	IP address of the default gateway	192.168.1.1
		Name Server	UINT32	IP address of the primary name server	0
		Name Server 2	UINT32	IP address of the secondary name server	0
		Domain Name	CHAR[32]	Default domain name	
6	Get	Host Name	CHAR[32]	Device name	

4.2.5.2 General Services

This object supports the following common services.

i Note

Changes made via “Set_Attribute_Single” do not take effect immediately!

Attributes that you change via the “Set_Attribute_Single” service do not take effect until the next time the product is restarted.

Table 23: Common Services

Service Code	Service Available		Service Name	Description
	Class	Instance		
0x01	Yes	Yes	Get_Attribute_All	Returns the content of all attributes
0x0E	Yes	Yes	Get_Attribute_Single	Returns the content of the respective attribute
0x10	No	Yes	Set_Attribute_Single	Modifies an attribute value

4.2.6 Ethernet Link Object

The Ethernet Link Object (Class 0xF6) contains link-specific counter and status information for an Ethernet 802.3 communication interface. Each device must support exactly one instance of the Ethernet Link Object for each Ethernet IEEE 802.3 communication interface. An Ethernet Link object instance for an internal interface, such as an internal port with an integrated switch, can also be used for the devices.

4.2.6.1 Instances

Table 24: Ethernet Link Object – Instance 0

Attribute ID	Access	Name	Data type	Description	Factory setting
1	Get	Revision	UINT16	Version of this object	4
2	Get	Max Instance	UINT32	Maximum number of instances	2
3	Get	Number of Instances	UINT32	Number of connections currently instantiated	2

Table 25: Ethernet Link Object – Instance 1 (Port 1)

Attribute ID	Access	Name	Data type	Description	Factory setting		
1	Get	Interface Speed	UINT32	Transmission rate	0x0000000A or 0x00000064		
2	Get	Interface Flags	UINT32	Interface configuration/status information		Dependent on ETHER-NET connection	
				Bit 0	Link Status		
				Bit 1	Half/full duplex		
				Bits 2 ... 4	Detection status		
				Bit 5	Manual settings require reset		
				Bit 6	Local hardware fault		
Bits 7 ... 31	Reserved						
3	Get	Physical Address	ARRAY of 6 UINTs	MAC address			
6	Get/ Set	Interface Control	STRUCT of:	Configuration of the physical interface			
		Control Bits	UINT16	Interface configuration bits			0x0001
				Bit 0	Automatic detection		
				Bit 1	Specification of duplex mode		
				Bits 2 ... 15	Reserved		
Forced Interface Speed	UINT16	Interface speed specified for the interface		0x000A or 0x0064			
7	Get	Interface Type	UINT8	Interface type		0x02 – Twisted Pair	
				Value 0	Unknown		
				Value 1	Internal interface, e.g., in the case of an integrated switch		
				Value 2	Twisted pair (e.g., 100BASE-TX)		
				Value 3	Glass fiber (e.g., 100BASE-FX)		
				Values 4 ... 256	Reserved		
8	Get	Interface Status	UINT8	Interface status			
				Value 0	Unknown		
				Value 1	Interface active and ready to send/receive		
				Value 2	Interface disabled		
				Value 3	Interface is testing		
				Values 4 ... 256	Reserved		
9	Get/ Set	Admin Status	UINT8	Administration status		0x01	
				Value 0	Reserved		
				Value 1	Enable interface		
				Value 2	Disable interface If this is the sole CIP interface, a request to disable is acknowledged with an error (error code 0x09).		
				Values 3 ... 256	Reserved		
10	Get	Interface Label	CHAR[]	Name of the interface	“ETH Port 1”		

Table 26: Ethernet Link Object – Instance 2 (Port 2)

Attribute ID	Access	Name	Data type	Description	Factory setting	
1	Get	Interface Speed	UINT32	Transmission rate	0x0000000A or 0x00000064	
2	Get	Interface Flags	UINT32	Interface configuration/status information		Dependent on ETHERNET connection
				Bit 0	Link Status	
				Bit 1	Half/full duplex	
				Bits 2 ... 4	Detection status	
				Bit 5	Manual settings require reset	
				Bit 6	Local hardware fault	
				Bits 7 ... 31	Reserved	
3	Get	Physical Address	ARRAY of 6 UINTs	MAC address		
6	Get/Set	Interface Control	STRUCT of:	Configuration of the physical interface		
		Control Bits	UINT16	Interface configuration bits		0x0001
				Bit 0	Automatic detection	
				Bit 1	Specification of duplex mode	
				Bits 2 ... 15	Reserved	
Forced Interface Speed	UINT16	Interface speed specified for the interface		0x000A or 0x0064		
7	Get	Interface Type	UINT8	Interface type		0x02 – Twisted Pair
				Value 0	Unknown	
				Value 1	Internal interface, e.g., in the case of an integrated switch	
				Value 2	Twisted pair (e.g., 100BASE-TX)	
				Value 3	Glass fiber (e.g., 100BASE-FX)	
				Values 4 ... 256	Reserved	
8	Get	Interface Status	UINT8	Interface status		
				Value 0	Unknown	
				Value 1	Interface active and ready to send/receive	
				Value 2	Interface disabled	
				Value 3	Interface is testing	
				Values 4 ... 256	Reserved	
9	Get/Set	Admin Status	UINT8	Administration status		0x01
				Value 0	Reserved	
				Value 1	Enable interface	
				Value 2	Disable interface If this is the sole CIP interface, a request to disable is acknowledged with an error (error code 0x09).	
				Values 3 ... 256	Reserved	
10	Get	Interface Label	CHAR[]	Name of the interface	"ETH Port 2"	

4.2.6.2 General Services

This object supports the following common services.

i Note

Changes made via “Set_Attribute_Single” do not take effect immediately!

Attributes that you change via the “Set_Attribute_Single” service do not take effect until the next time the product is restarted.

Table 27: Common Services

Service Code	Service Available		Service Name	Description
	Class	Instance		
0x01	Yes	Yes	Get_Attribute_All	Returns the content of all attributes
0x0E	Yes	Yes	Get_Attribute_Single	Returns the content of the respective attribute
0x10	No	Yes	Set_Attribute_Single	Modifies an attribute value

4.2.7 Device Parameter Object

The Device Parameter object (class 0x82) provides access to the parameters and information of a lower-level device. Only instance ID 1 is implemented for this object.

4.2.7.1 General Device Parameters of Lower-Level Devices

The product uses the following general parameters of the lower-level device.

Device Identification

Table 28: General Device Parameters – Device Identification

Attribute ID	Access	Data type	Description
2	Get	UINT32	Item Number
4	Get	UINT32	Item number extension
8	Get	UINT32	Consecutive number (“high word”)
10	Get	UINT32	Consecutive number (“low word”)
12	Get	UINT16	Firmware version (major)
13	Get	UINT16	Firmware version (minor)
14	Get	UINT16	Firmware version (bug fix)
15	Get	UINT16	Hardware version
20	Get	CHAR[32]	Item description
36	Get/Set	CHAR[32]	Device name
52	Get/Set	CHAR[32]	Customer information (1)
68	Get/Set	CHAR[32]	Customer information (2)
84	Set	CHAR[8]	Password
92	Get/Set	UINT16	Password level

„Password“ Parameter

i Note

The device must be locked manually!

After the lower-level device is unlocked, it is not automatically relocked. The device lock must be performed manually.

The parameter is used in big-endian format. Only ASCII characters may be used (e.g., for password “123,” a message with the following hexadecimal values must be sent: 31 32 33.)

„Password protection level“ Parameter

The “Password Level” parameter controls the behavior of the lower-level device in terms of password protection. There are four password levels:

- Password level 0 (value 0): No parameters are password protected
- Password level 1 (value 1): All parameters are write-protected
- Password level 2 (value 2): All parameters are read- and write-protected
- Password level 3 (value 3): All parameters are read- and write-protected In addition, process data outputs (e.g., “Switch product on and off” or “Activate digital output”) are write-protected.

i Note

Set the password first!

When parameterizing the password, the parameter “Password” must be set first, afterwards the parameter “Password Protection Level” must be configured.

Table 29: General Device Parameters – “Password Level” Parameter

Password level	Parameter: Write Protection	Parameter: Read Protection	Process Data: Write Protection	Process Data: Read Protection
0	No	No	No	No
1	Yes	No	No	No
2	Yes	Yes	No	No
3	Yes	Yes	Yes	No

General Device Parameters

Table 30: General Device Parameters – Modbus

Attribute ID	Access	Data type	Description	
122	Get/Set	UINT16	Device address	
124	Get/Set	UINT32	Baud rate This parameter can be used to set the baud rate. The options are as follows:	
			Value	Baud Rate
			4800	4800 baud
			9600	9600 baud
			19200	19200 baud
			38400	38400 baud
			57600	57600 baud
			115200	115200 baud
			230400	230400 baud
560800	560800 baud			
126	Get/Set	UINT16	Data bits The options are as follows:	
			Value	Data Bit
			0	7
1	8			
127	Get/Set	UINT16	Stop bits The options are as follows:	
			Value	Stop Bit
			0	1
			1	0.5
			2	2.5
3	1.5			
128	Get/Set	UINT16	Parity The options are as follows:	
			Value	Parity
			0	None
			1	Even
2	Odd			
129	Get/Set	UINT16	Response delay (unit: ms)	
130	Get/Set	UINT16	Data format The options are as follows:	
			Value	Data Format
			0	Big-endian (B0, B1, B2, B3)
			1	Middle-endian (B2, B3, B0, B1)
2	Little-endian (B3, B2, B1, B0)			

4.2.7.2 Device Parameters of the WAGO Pro 2 Power Supply

The following parameters of the WAGO Pro 2 Power Supply can be edited via the product.

DC Output

Table 31: Parameters – DC Output

Attribute ID	Access	Data type	Description	
136	Get/Set	UINT16	Output voltage (unit: mV)	
137	Get/Set	UINT16	Warning threshold (unit: mA)	
138	Get/Set	UINT16	Bit 0	Switch output on
			Bit 1	"Active droop" parallel switching mode
			Bit 2	Overload threshold enabled
			Bit 3	Enable switching the DC output on and off via cyclic process data
			Bits 4 ... 5	Reserved
			Bit 6 ¹	Constant current
			Bit 7 ¹	Constant current with latching shutdown
			Bit 8 ¹	Hiccup mode
			Bit 9 ¹	Electronic circuit breaker
			Bits 10 ... 11	Reserved
			Bit 12	Latching shutdown on thermal overload
			Bit 13	PowerBoost
			Bit 14	TopBoost
Bit 15	Reserved			
139	Get/Set	UINT16	Switch-on delay (unit: ms)	

¹ At least one bit must be set, and the bits are mutually locked.

Electronic Circuit Breaker Mode

Table 32: Parameters – Electronic Circuit Breaker Mode

Attribute ID	Access	Data type	Description
148	Get/Set	UINT16	Trip current (unit: mA)
149	Get/Set	UINT16	Trip delay (unit: ms)

Signaling – Digital Input

Table 33: Parameter – Signaling – Digital Input

Attribute ID	Access	Data type	Description	
168	Get/Set	UINT16	Bit 0	Switch power supply on and off
			Bits 1 ... 9	Reserved
			Bit 10 ¹	Inversion
			Bit 11 ¹	Function on edge change (0 to 1)
			Bit 12 ¹	Function on edge change (1 to 0)
			Bits 13 ... 15	Reserved

¹ All bits can be 0 and are mutually locked.

Signaling – Digital Output

Table 34: Parameter – Signaling – Digital Output

Attribute ID	Access	Data type	Description	
176	Get/Set	UINT16	Bit 0	DC status OK
			Bit 1	Overload threshold exceeded
			Bit 2	Electronic circuit breaker tripped
			Bit 3	Latching shutdown occurs

Attribute ID	Access	Data type	Description	
			Bit 4	Activation of the readout function of the digital output via the process data
			Bit 5	Switching digital output on and off
			Bits 6 ... 9	Reserved
			Bit 10	Inversion
			Bits 11 ... 15	Reserved

System

Table 35: Parameters – System

Attribute ID	Access	Data type	Description	
189	Get/Set	UINT16	Bit 0 ¹	Behavior when power applied: Previous state restored
			Bit 1 ¹	Behavior when power applied: DC output remains switched off
			Bit 2 ¹	Behavior when power applied: DC output switched on
			Bit 3	Switch-on delay enabled
			Bits 4 ... 5	Reserved
			Bit 6	Enable button lock
			Bit 7	Lock resetting to factory settings
			Bits 8 ... 9	Reserved
			Bit 10	Inversion
			Bits 11 ... 15	Reserved

¹ These bits are mutually locked.

4.2.7.3 General Services

This object supports the following common services.

Table 36: Common Services

Service Code	Service Available		Service Name	Description
	Class	Instance		
0x0E	Yes	Yes	Get_Attribute_Single	Returns the content of the respective attribute
0x10	No	Yes	Set_Attribute_Single	Modifies an attribute value

4.2.8 Module Parameter Object

The Module Parameter object (Class 0x78) provides access to the internal module parameters and module information. Only instance ID 1 is implemented for this object.

Cross-Device Information for Identification

Table 37: Internal Module Parameters – Cross-Device Information for Identification

Attribute ID	Access	Data type	Description	Factory setting
2	Get	UINT32	Module item number	0x28579023
8	Get	UINT32	Consecutive number (“high word”)	
10	Get	UINT32	Consecutive number (“low word”)	
12	Get	UINT16	Firmware version (major)	
13	Get	UINT16	Firmware version (minor)	
14	Get	UINT16	Firmware version (bug fix)	
15	Get	UINT16	Hardware version	
20	Get	CHAR[34]	Fixed item description of the device	“EtherNet/IP Communication Module”
37	Get/Set	CHAR[34]	Location name	
54	Get/Set	CHAR[34]	Function name	
71	Get/Set	CHAR[34]	Customer information	

General ETHERNET Settings

Table 38: Internal Module Parameters – General ETHERNET Settings

Attribute ID	Access	Data type	Description	Value Limits		
				Factory setting	Min.	Max.
106	Get	CHAR[6]	MAC address of the communication module			
109	Get/Set	CHAR[4]	IP address of the communication module	192.168.1.17		
111	Get/Set	CHAR[4]	Subnet mask of the communication module	255.255.255.0		
113	Get/Set	CHAR[4]	Gateway address	192.168.1.1		
116	Get/Set	UINT16	Enables “fast aging” (0 = off, 1 = on)	0		
118	Get/Set	UINT16	Enables WBM via HTTP (0 = off, 1 = on)	1	0	1
119	Get/Set	UINT16	Enables WBM via HTTPS	1	0	1
120	Get/Set	UINT16	Enables SNTP (0 = off, 1 = on)	0	0	1
124	Get/Set	CHAR[4]	IP address of the SNTP server	192.168.1.109		

Switch Settings for Channel 1

Table 39: Internal Module Parameters – Switch Settings for Channel 1

Attribute ID	Access	Data type	Description	Value Limits		
				Factory setting	Min.	Max.
236	Get/Set	UINT16	Enables “Autonegotiation” mode (0 = off, 1 = on)	1	0	1
237	Get/Set	UINT16	Forces 100 MB connection (0 = off, 1 = on)	1	0	1
238	Get/Set	UINT16	Forces full duplex connection (0 = off, 1 = on)	1	0	1

Attribute ID	Access	Data type	Description	Value Limits		
				Factory setting	Min.	Max.
240	Get/Set	UINT16	Enables BroadcastStormProtection (0 = off, 1 = on)	0	0	1

Switch Settings for Channel 2

Table 40: Internal Module Parameters – Switch Settings for Channel 2

Attribute ID	Access	Data type	Description	Value Limits		
				Factory setting	Min.	Max.
248	Get/Set	UINT16	Enables "Autonegotiation" mode (0 = off, 1 = on)	1	0	1
249	Get/Set	UINT16	Forces 100 MB connection (0 = off, 1 = on)	1	0	1
250	Get/Set	UINT16	Forces full duplex connection (0 = off, 1 = on)	1	0	1
252	Get/Set	UINT16	Enables BroadcastStormProtection (0 = off, 1 = on)	0	0	1

Note

Restart after adjusting switch and ETHERNET settings!

After settings are modified on this page, the product must be restarted with **[Reboot Module]** or by power cycling¹⁾ it.

1) The device must be disconnected from the supply voltage for at least five seconds.

Date

Table 41: Internal Module Parameters – Date

Attribute ID	Access	Data type	Description	Value Limits		
				Factory setting	Min.	Max.
260	Get/Set	UINT8	Year	0	0	99
	Get/Set	UINT8	Month	1	1	12
	Get/Set	UINT8	Day	1	1	31

Time

Table 42: Internal Module Parameters – Time

Attribute ID	Access	Data type	Description	Value Limits		
				Factory setting	Min.	Max.
262	Get/Set	UINT8	Hours	0	0	23
	Get/Set	UINT8	Minutes	0	0	59
	Get/Set	UINT8	Seconds	0	0	59
264	Get/Set	UINT16	Time zone	0	-12	12
265	Get/Set	UINT16	Synchronization mode (1 = off, 2 = read time from the lower-level device, 4 = write time from module, 8 = update time with SNTP)	1		

This object supports the following common services.

Table 43: Common Services

Service Code	Service Available		Service Name	Description
	Class	Instance		
0x0E	Yes	Yes	Get_Attribute_Single	Returns the content of the respective attribute
0x10	No	Yes	Set_Attribute_Single	Modifies an attribute value

4.2.9 Measurement Data Object

The Measurement Data object (Class 0x8C) allows the events and measured values of a lower-level device to be read. Only instance ID 1 is implemented for this object.

4.2.9.1 Events and Measured Values

The object outputs the WAGO-specific events and measured values listed below.

Process Output Data

Table 44: Events and Measured Values – Process Input Data

Attribute ID	Access	Data type	Description
0	Get	UINT16	Output voltage (unit: mV)
1	Get	UINT16	Output current (unit: mA)

Status Messages

Table 45: Events and Measured Values – Status Messages

Attribute ID	Access	Data type	Description	
2	Get	UINT16	Bit 0	DC status OK
			Bit 1	Overtemperature
			Bit 2	No output voltage
			Bit 3	Short circuit at output
			Bit 4	Status at digital input

Warnings

Table 46: Events and Measured Values – Warnings

Attribute ID	Access	Data type	Description	
3	Get	UINT16	Bit 0	Undervoltage at output
			Bit 1	Overvoltage at output
			Bit 2	Overload
			Bit 3	Configurable overload threshold exceeded
			Bit 4	Configurable operating hours reached
			Bit 5	TopBoost output
			Bit 6	PowerBoost output
			Bit 7	Higher device temperature
			Bit 8	-

Error

Table 47: Events and Measured Values – Errors

Attribute ID	Access	Data type	Description	
4	Get	UINT16	Bit 0	Overtemperature, device switched off
			Bit 1	No output voltage
			Bit 2	Short circuit at output
			Bit 3	Circuit breaker tripped

Power/Energy

Table 48: Events and Measured Values – Power/Energy

Attribute ID	Access	Data type	Description
6	Get	UINT32	Output power (unit: W)
8	Get	UINT32	Output level of previous second (unit: Ws)
10	Get	UINT32	Output level of previous minute (unit: Ws)
12	Get	UINT32	Output level of previous hour (unit: Wh)

4.2.9.2 General Services

This object supports the following common services.

Table 49: Common Services

Service Code	Service Available		Service Name	Description
	Class	Instance		
0x0E	Yes	Yes	Get_Attribute_Single	Returns the content of the respective attribute

4.3 MQTT

“Message Queuing Telemetry Transport” (MQTT) defines an open network protocol that is the preferred choice for exchanging data between IoT (“Internet of Things”) devices. The product is an MQTT client that can be connected to a local broker.

The product supports the following features:

- MQTT protocol version: 3.1.1
- Quality of service level: 1
- Unencrypted port: 1883
- Encrypted port: 8883
- TLS version: 1.3

For configuration with a broker, see [🔗 Configuration of Communication with Broker \[▶ 63\]](#).

4.3.1 Connection Status

The following table shows the possible states of the connection status.

Table 50: MQTT Connection Status

Status	Description	Trigger (Preceding Action)
Disabled	MQTT communication is disabled	MQTT connection is configured to Disable
Connecting	Communication is being established	MQTT connection is configured to Enable
Connected	Communication has been established	
No certificate found	No certificate found for encrypted communication	Encrypted communication is started even though no certificate has been uploaded
Certificate verification failed	Certificate verification failed	An invalid certificate is uploaded or is already in internal memory (may be due to incorrect module time/ date)
New certificate detected, reboot required	New certificate was detected, restart required	An existing certificate is replaced with a new one and encrypted communication is restarted

4.3.2 Data Exchange

Process data of a lower-level device can be read and written via the MQTT protocol. The access operations can use JSON format or binary format. For the binary format, you can choose between big-endian and little-endian.

In the following tables, the term “*value*” serves as a placeholder. When data is read out, the current value appears.

The byte order depends on the data format selected.

The following process data can be read out in JSON format (communication module “*Publish*” to the broker):

Table 51: Reading Out Process Data in JSON Format

No.	Description	JSON Format
1	Status of the connection to the lower-level device	"Module Status" : { "Connection to device O.K." : " <i>value</i> " }

No.	Description	JSON Format
2	Output voltage	"Voltage" : { "Value" : "value", "Unit" : "mV" }
3	Output current	"Current" : { "Value" : "value", "Unit" : "mA" }
4	Status	"Device Status" : { "Status DC O.K." : "value", "Status overheating" : "value", "No output voltage" : "value", "Output short circuit" : "value", "Status of digital input" : "value" }
5	Warnings	"Warnings" : { "Output under-voltage" : "value", "Output over-voltage" : "value", "Overload" : "value", "Adjustable output current limit exceeded" : "value", "Adjustable operating hour limit exceeded" : "value", "Top boost supplied" : "value", "Power Boost supplied" : "value", "High device temperature" : "value", "Digital input active" : "value" }
6	Errors	"Errors" : { "Overheating, device switched off" : "value", "No output voltage" : "value", "Output short circuit" : "value", "Electronic circuit breaker tripped" : "value" }
7	Control word	"Output" : { "Device standby" : "value" ¹⁾ , "Digital out on" : "value" }

1 Not yet supported by the WAGO Pro 2 Power Supply

The following process data can be written in JSON format (communication module “Subscribe” from the broker):

Table 52: Writing Process Data in JSON Format

No.	Description	JSON Format
1	Control word	"Output" : { "Device standby" : "value", ¹⁾ "Digital out on" : "value" }

1 Not yet supported by the WAGO Pro 2 Power Supply

The following process data can be read out in binary format:

Table 53: Reading Out Process Data in Binary Format

No.	Data type	Description	
1	UINT16	Module status	
		Bit 0	Communication with lower-level device OK
2	UINT16	Output voltage (unit: mV)	
3	UINT16	Output current (unit: mA)	
4	UINT16	Status	
		Bit 0	DC status OK
		Bit 1	Overtemperature
		Bit 2	No output voltage
		Bit 3	Short circuit at output
		Bit 4	Status at digital input
5	UINT16	Warnings	
		Bit 0	Undervoltage at output
		Bit 1	Overvoltage at output
		Bit 2	Overload
		Bit 3	Configurable overload threshold exceeded
		Bit 4	Configurable operating hours reached
		Bit 5	TopBoost output
		Bit 6	PowerBoost output
		Bit 7	Higher device temperature
Bit 8	Digital input active		
6	UINT16	Error	
		Bit 0	Overtemperature, device switched off
		Bit 1	No output voltage
		Bit 2	Short circuit at output
		Bit 3	Circuit breaker tripped
7	UINT16	Control word	
		Bit 0	Device standby ¹
		Bit 1	Digital output on

¹ Not yet supported by the WAGO Pro 2 Power Supply

The following process data can be written in binary format:

Table 54: Writing Process Data in Binary Format

Byte No.	Data type	Description	
1	UINT16	Control word	
		Bit 0	Device standby ¹
		Bit 1	Digital output on

¹ Not yet supported by the WAGO Pro 2 Power Supply

4.3.3 Application Examples

The following are application examples for connecting the communication module and the WAGO Pro 2 Power Supply to other controllers.

Raspberry Pi as MQTT Broker

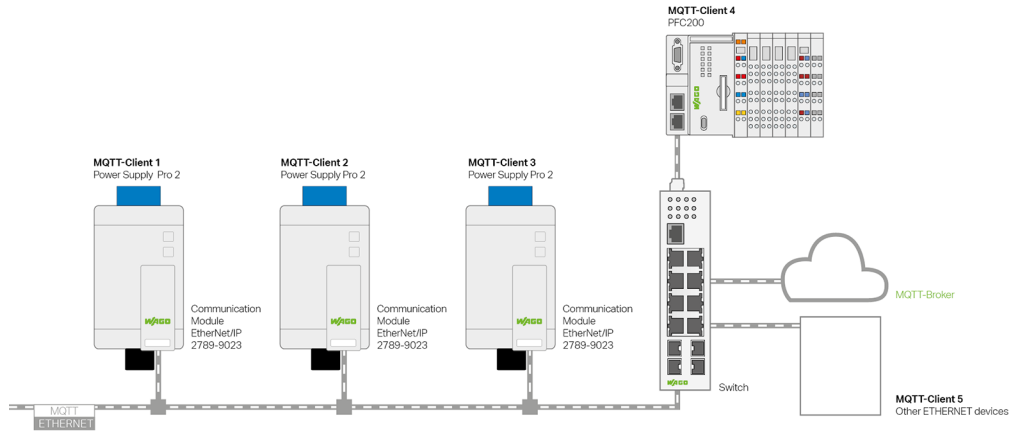


Figure 5: Raspberry Pi as MQTT Broker

- The product serves as an MQTT client.
- A WAGO PFC200 (e.g., item no. 750-8212) serves as an MQTT client for integrating the communication modules into CODESYS or e!COCKPIT.
- Any computer (e.g., a Raspberry Pi with a Mosquitto MQTT broker) can serve as the MQTT broker.

WAGO PFC200 as MQTT Broker

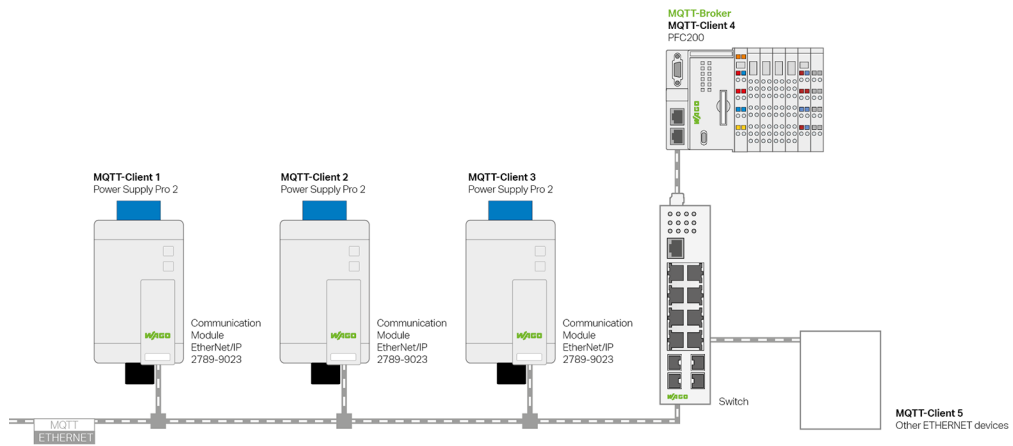


Figure 6: WAGO PFC 200 as MQTT Broker

- The product serves as an MQTT client.
- A WAGO PFC200 (e.g., item no. 750-8212) serves as MQTT client and MQTT broker. The PFC controller allows the communication modules to be integrated into CODESYS or e!COCKPIT and serves as a server/broker at the same time.

Transport and Storage

The original packaging offers optimal protection during transport and storage.

- Store the product in suitable packaging, preferably the original packaging.
- Only transport the product in suitable containers/packaging.
- Make sure the product contacts are not contaminated or damaged during packing or unpacking.
- Observe the specified ambient climatic conditions for transport and storage.

Installation and Removal

! NOTICE

Do not cover the ventilation openings!

Covered ventilation openings can lead to overheating of the product.

- Keep all ventilation openings clear!

The letters shown in parentheses refer to positions in figure “View” in [View \[▶ 12\]](#).

i Note

Mounting positions

The nominal mounting position is (see also figure “View” in [View \[▶ 12\]](#)): front side facing forwards, marking legible, bottom ventilation openings (b) facing upwards and downwards

Mounting

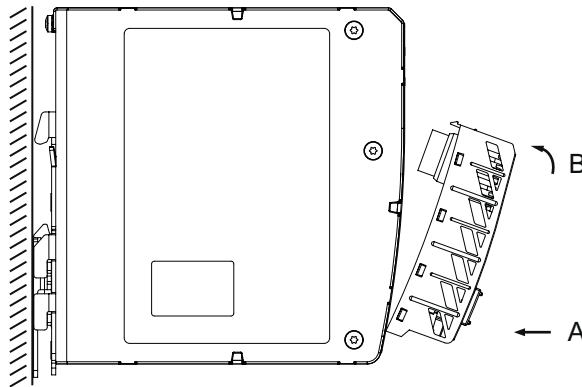


Figure 7: Mounting

Install the product by snapping it onto the WAGO Power Supply Pro 2 (see figure “Installation”):

1. Remove the cap from the communication interface on the WAGO Power Supply Pro 2.
2. Keep the cap in a safe place so that you can cover the communication interface again when this interface is not required.
3. Remove the mounted marker carrier from the WAGO Power Supply Pro 2.
4. Insert the product with the lower latches into the lower mounting slots of the WAGO Power Supply Pro 2 [A].
5. Slide the product toward the communication interface [B] until the top latches latch into the top mounting slots.
6. Verify that the product is snapped on properly.

Removal

! NOTICE

Material damage due to hot swapping!

Hot swapping the product leads to increased abrasion of the contacts. Resulting in a shorter product life time.

- Only remove the product when it is switched off.

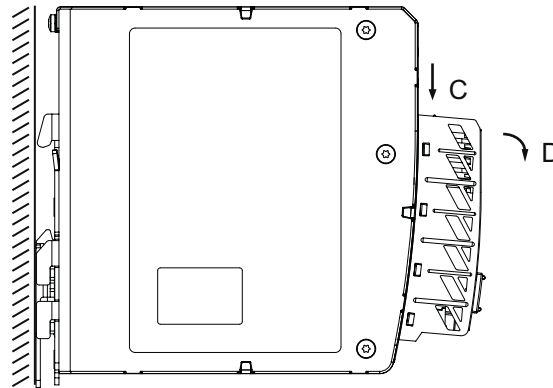


Figure 8: Removal

1. Press the top locking tab (a) of the product [C].
2. Pivot the product to remove it from the WAGO Power Supply Pro 2 [D].

! NOTICE

Avoid electrostatic discharge!

The products are equipped with electronic components that you may destroy by electrostatic discharge when you touch. Please observe the safety precautions against electrostatic discharge in accordance with EN 61340-5-1/-3. Pay attention while handling the products to good grounding of the environment (persons, job and packing).

Commissioning

7.1 Setting an IP address

7.1.1 Assigning an IP Address Using DHCP

- ✓ Snap the product onto a lower-level device.
 - ✓ Connect the product to a computer via a network cable and integrate it into a network.
 - ✓ Supply the lower-level device with power.
 - ✓ If there is a DHCP server in the network:
 - Assign the network settings to the product.
 - ✓ When the product is delivered, dynamic IP address assignment via the “Dynamic Host Configuration Protocol” (DHCP) is enabled by default.
 - When the DHCP protocol is enabled, make sure a DHCP server is always present.
 - ✓ If the IP address was assigned via DHCP:
 - Determine this address via the settings or the output of the respective DHCP server, for example via the output of “Open DHCP.”
- ⇒ Configuration type: static IP address
- ⇒ IP address: 192.168.1.17
- ⇒ Gateway address: 192.168.1.1

i Note

Two DHCP servers in one network can cause total network failure!

To prevent network failure, never connect a PC on which a DHCP server is installed to a global network. In larger networks, there is usually already a DHCP server that can cause collisions and subsequent network failure.

i Note

Assign a fixed IP address to the DHCP server and ensure that a common subnet exists!

Note that the DHCP server must have a fixed IP address and that the product and DHCP server must be in the same subnet.

i Note

IP addresses obtained via DHCP server are only valid temporarily!

Note that an IP address obtained via a DHCP server is only valid for a limited period of time. If the DHCP server is not available after the service life has elapsed, the fieldbus node releases the IP address and can then no longer be reached!

7.1.2 Setting a Static IP Address

To use the IP address permanently, you can switch the addressing to “static.” The following options are available for this:

- Setting the IP address via the WBM
- Setting the default IP address with the reset button
- Setting the IP address via the Modbus command

Setting the IP Address via the WBM

1. Open the WBM (Web-Based Management) of the communication module in a browser.
2. Switch to the **Module Settings > Network** page of the WBM.
3. In the **Ethernet Settings** area, you can make the required network settings.

Figure 9: Module Settings > Network

Note

The communication module must be restarted for the settings to be applied.

4. To restart, press the **[Start]** button in the **Reboot** section of the **Module Settings > System** page of the WBM, or power cycle your system.

Figure 10: Module Settings > System

Setting the Default IP Address with the Reset Button

i Note

If you no longer have the IP address of the module, you can reset the network settings with the reset button on the module.

1. Hold the reset button down for eight seconds until the “COM OK” LED lights up briefly.
 2. Release the reset button.
- ⇒ The product reboots, and the following network settings are made:
- Configuration type:** static IP address
 - IP address:** 192.168.1.17
 - Gateway address:** 192.168.1.1

Setting the IP Address via Modbus Command

- Write to the corresponding addresses using Modbus FC10 Internal Module Parameters.

Operation

8.1 Operating via Reset Button

The reset button can be used to reset the product.

The following settings options are available:

Table 55: Using the Reset Button

Settings Options	Description	Signaling via Visual Status Display
Hold reset button down for eight seconds	Disables DHCP and sets the IP address to 192.168.1.17	COM OK flashes once
Hold reset button down for ten seconds	Resets the product to the factory settings	ERR flashes at 16 Hz

Configuration

9.1 Configuring with WBM

Using the Web-Based Management (WBM), you can view parameters and measured values of the communication module and the lower-level device and make changes via a Web browser.

9.1.1 Logging In

If the lower-level device is password-protected, one of the following messages appears, depending on the password level:

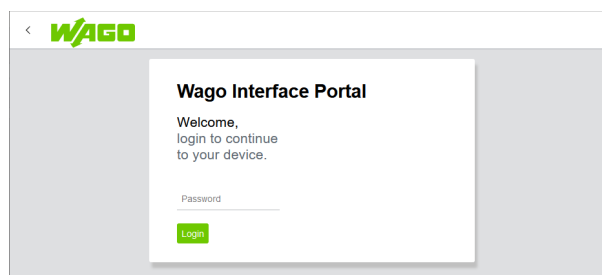


Figure 11: Login with Read/Write Protection

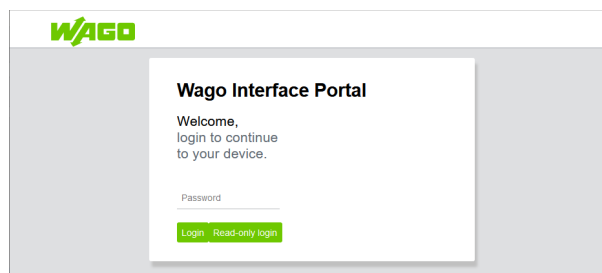


Figure 12: Login with Read Protection

If the lower-level device is read and write protected, it must always be unlocked with a password (see figure “Login with Read/Write Protection”). With read protection, it is possible to either log in with **[Read-Only Login]** without entering a password or unlock it completely by entering the correct password.

9.1.2 Menu Page

- ✓ The lower-level device is not password-protected
 - OR
 - ✓ Logging in with a password is possible
 - Log in.
- ⇒ The menu page of the WBM appears with the pages offered.

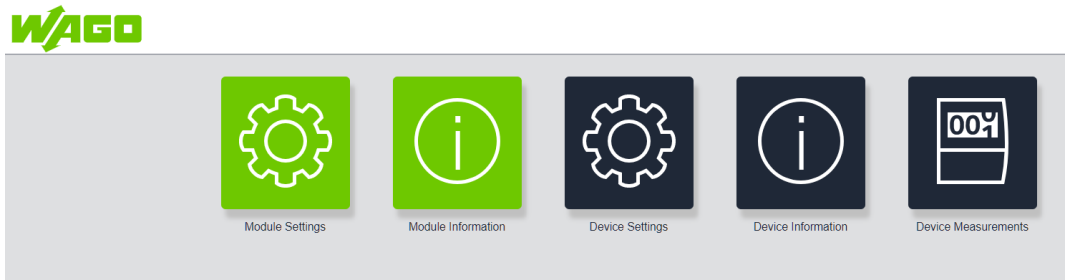


Figure 13: Menu Page

On the menu page, you will see tiles offering the following entry points:

- Module Settings
- Module Information
- Device Settings
- Device Information
- Device Measurements

9.1.3 Module Settings

System

System	MQTT	EtherNet/IP	Network	Parameter Management	Switch settings
Date / Time					
Date (YYMMDD)	00 . 01 . 01 <input type="button" value="Set date from PC"/>				
Time (hhmmss)	00 . 00 . 00 <input type="button" value="Set time from PC"/>				
Date (YYMMDD)	00.01.01				
Time (hhmmss)	01.22.56				
<input checked="" type="radio"/> Enable SNTP					
SNTP-Server	192 . 168 . 1 . 109				
SNTP update time	60 sec <small>(min: 0, max: 604800)</small>				
Time zone UTC	0 h <small>(min: -12, max: 12)</small>				
Firmwareupdate					
Start firmware update of module	<input type="button" value="Start"/>				
<small>NOTE: Firmware update is only possible in HTTP-mode, if you are in HTTPS please switch to HTTP for activating.</small>					
Reboot					
Reboot module	<input type="button" value="Start"/>				
Factory Reset					
Factory Reset	<input type="button" value="Start"/>				

Figure 14: Module Settings > System

Date / Time: Here you can set the module's date and time.

- Manual
- Use current PC time
- Get the time from an SNTP server

i Note

Restart after configuring SNTP!

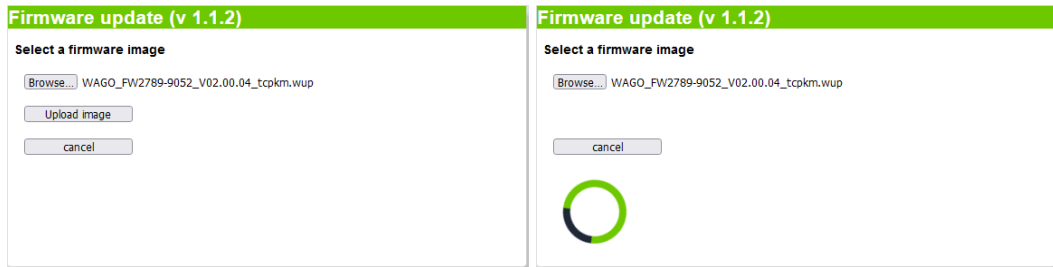
After SNTP is configured, the product must be restarted with **[Reboot Module]** or by power cycling it.

Firmware Update: You can also update the module’s firmware. Clicking the **[Start]** button takes you out of the application and launches the internal firmware loader.

i Note

Please note the version of the firmware loader!

Below, exemplary images of a particular version are used. Therefore, note that your WBM interface differs depending on the version you're using. You can see the version of the firmware loader in brackets on the WBM page "Firmware update", e.g. "(v 1.1.2)".



i Note

Notes on updating the firmware

Please note that the module firmware can only be updated via the HTTP protocol. For this purpose, the website must be accessed via HTTP.

While the firmware loader is active, module tasks cannot be executed.

If the firmware loader is interrupted during the update process, the module remains in firmware loader mode permanently until a firmware image is loaded.

After the firmware update ends, it may be necessary to manually refresh the page.

Reboot: module restart is necessary after network settings are modified

Factory Reset: resets the module parameters to the factory settings

MQTT

You can change the MQTT settings here; see [MQTT \[▶ 41\]](#).

Figure 15: Module Settings > MQTT

- **ID:** client ID used for connecting to the broker; can only be used once if multiple clients are used
- **User/Password:** If the broker requires authentication with a username and password, these can be configured here
- **Subscribe topic:** topic used by the communication module to receive messages from the broker
- **Publish topic:** topic for which the communication module will send messages to the broker
- **Publish interval:** interval at which the communication module sends the messages
- **Keep Alive:** time interval for checking the availability of the subscribers
- **IP-Address:** IP address of the broker Certificate Upload for loading your MQTT certificates; see [User Certificates \[▶ 67\]](#).

i Note

Set Date / Time before certificate upload!

Before a certificate is uploaded, the settings for **Date / Time** must be set under **[Module Settings > System]**.

EtherNet/IP

Figure 16: Module Settings > EtherNet/IP

- **Encapsulation Inactivity Timeout:** time interval for closing an inactive connection

Network

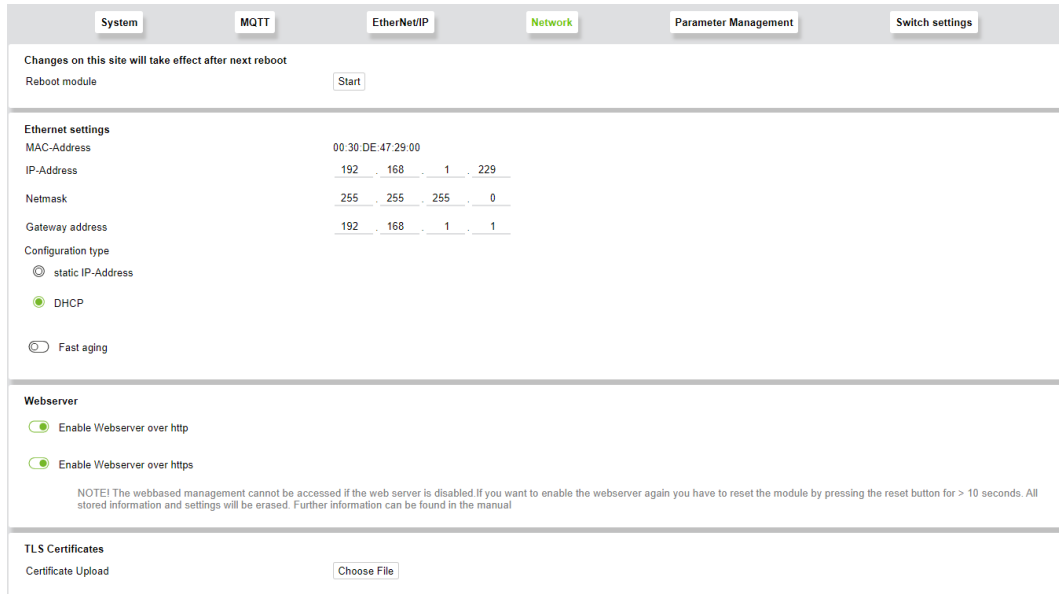


Figure 17: Module Settings > Network

i Note

Restart after modifying the network settings!

After settings are modified on this page, the product must be restarted with **[Reboot Module]** or by power cycling it.

- **Ethernet settings:** Setting the network parameters and addressing type
- **Webserver:** Here you can switch the HTTP and HTTPS protocols on or off

i Note

Re-enabling Webserver access

Disabling the Webserver closes ports 80 and 443; the module is then no longer accessible via Web browser. To re-enable access via the Webserver, you must hold the reset button on the module down physically for longer than ten seconds. This resets the module to the factory settings, or you must set Attribute ID 118 for HTTP or 119 for HTTPS to 1 via EtherNet/IP.

- **TLS Certificates:** Loading your own TLS certificates for the HTTPS protocol; [User Certificates \[p 67\]](#).

Parameter Management

Here you can save the current settings of the module and lower-level device and transfer them to other devices of the same type.

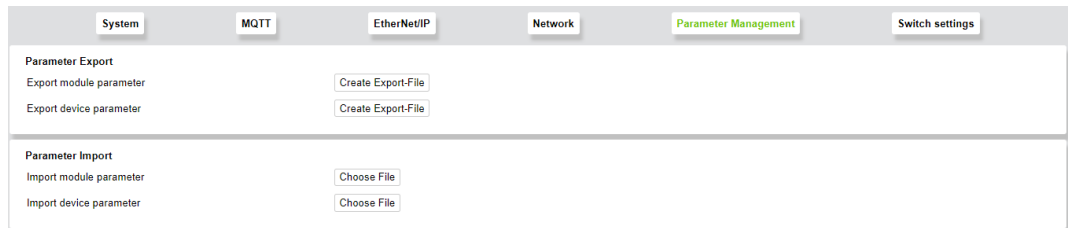


Figure 18: Module Settings > Parameter Management

- **Parameter Export:** module and device parameter settings can be exported
- **Parameter Import:** module and device parameters can be imported

Switch Settings

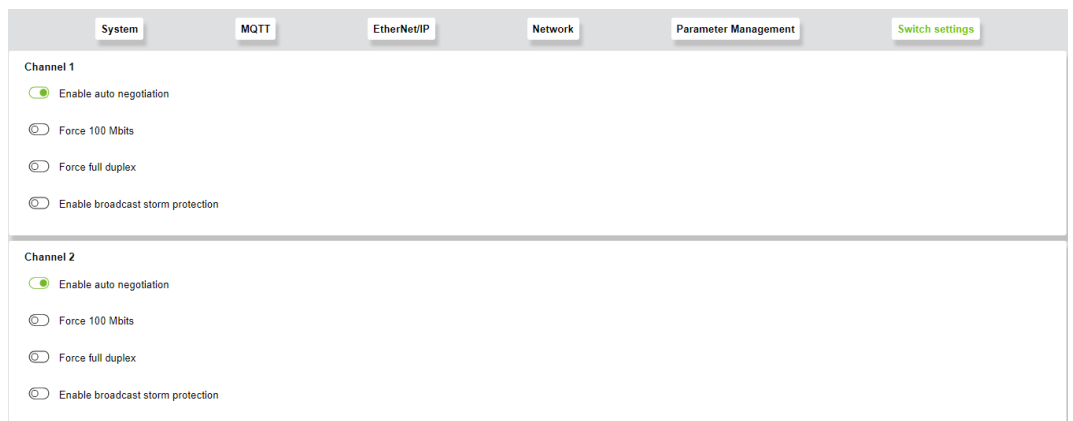


Figure 19: Module Settings > Switch settings

- **Enable Autonegotiation:** Autonegotiation allows the UTP (Unshielded Twisted Pair) link partners to select the best common operating mode in accordance with Clause 28 of the IEEE 802.3u specification. With autonegotiation, the link partners share their capabilities with each other over the link.
- **Force 100 Mbits:** forces connection via 100 Mbit
- **Force Full Duplex:** forces connection using full duplex
- **Enable Broadcast Storm Protection:** This option can be used to protect the switch system from receiving too many broadcast packets. Since the broadcast packets are forwarded to all ports except the source port, this can tie up an excessive number of switch resources (bandwidth and available space in the send queues). The module can optionally take multicast packets into account for storm control.

See also

- 📄 [MQTT \[▶ 41\]](#)
- 📄 [User Certificates \[▶ 67\]](#)
- 📄 [User Certificates \[▶ 67\]](#)
- 📄 [User Certificates \[▶ 67\]](#)

9.1.4 Module Information

General

This displays all the module information and indicates the status of the connection to the lower-level device:

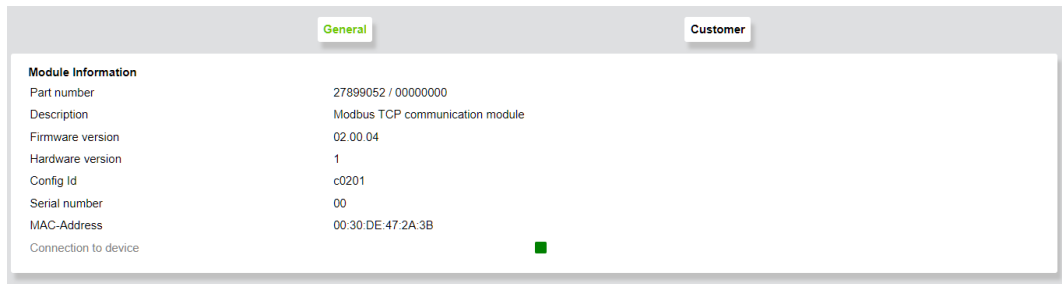


Figure 20: Module Information > General

- **Connection to Device:** Green means the connection is established; red means the connection is disrupted.

Customer

Users can enter system and location information here:

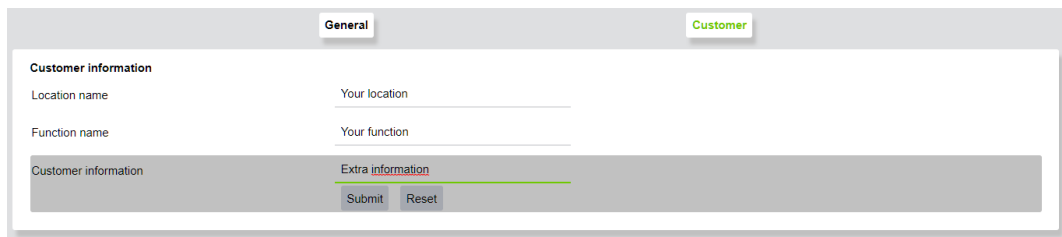


Figure 21: Module Information > Customer

9.1.5 Device Settings

The individual menu pages of the **Device Settings** are shown below. For a detailed description of each function, see **Configuring** in the

- **Product Manual** of the Pro 2 Power Supply used

DC Output

All parameters are read from the lower-level device and displayed on the **Device Parameter** page.

Figure 22: Device Settings > DC Output

- **General:** Here you can make general settings concerning how **DC output** switches on or off, and with **Output On**, the current output voltage is also displayed.
- **Overload Behavior:** Here you can specify how the product should behave in case of overload.

Signalization

i Note

Navigation is valid from firmware version 1.5.17!

The WBM interface in this form is displayed from firmware version 1.5.17. For older versions, the password settings can be found under **[Device Settings] > [System]** and the Modbus settings cannot yet be configured via WBM.

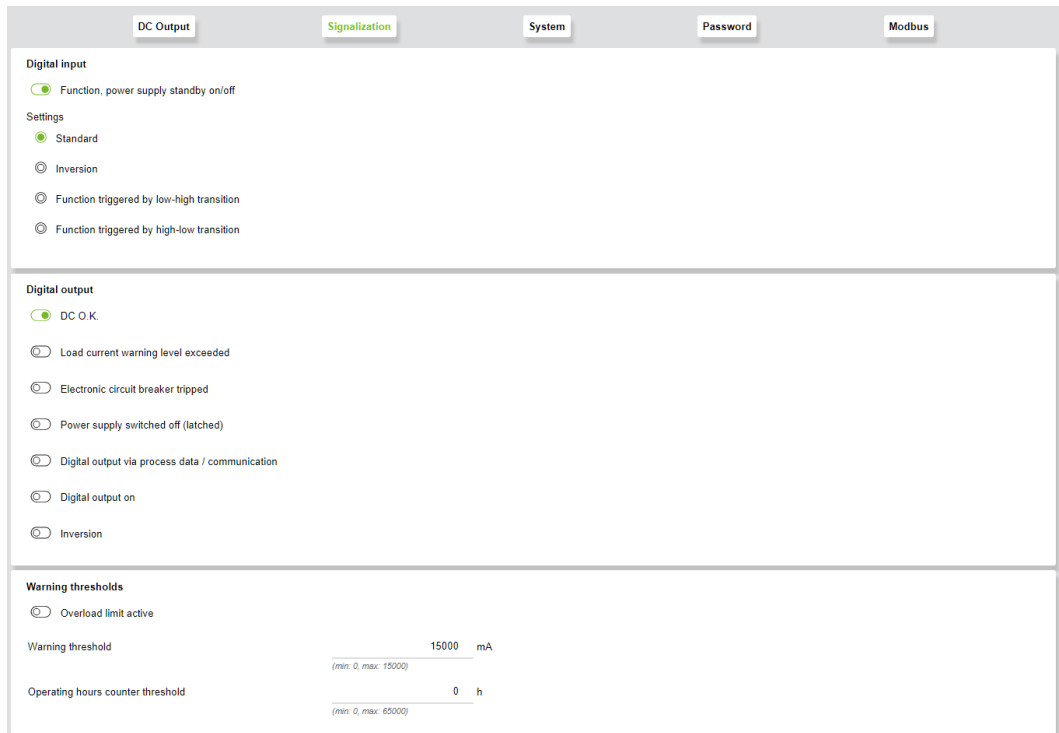


Figure 23: Device Settings > Signalization

- **Digital Input:** Here you can switch the power supply on and off and make additional settings.
- **Digital Output:** This contains various setting options for the digital output; **Digital Output On** and **Inversion** are locked and cannot be selected at the same time as other settings.
- **Warning Thresholds:** Here you can configure warning threshold settings.

System

The screenshot shows the 'System' configuration page with the following sections:

- Power on behavior:** Radio buttons for 'Restore previous status' (selected), 'DC output to be switched on', and 'DC output remains switched off'. A checkbox for 'Switch-on delay active' is also present. Below is a 'Switch-on delay' input field set to '0 ms' with a range of '(min: 0, max: 60000)'.
- User interface:** Two checkboxes: 'Disable reset to factory settings' and 'Activate key lock'.
- Date / Time:** Fields for 'Date (YYMMDD)' and 'Time (hhmmss)' with 'Set from PC' buttons. Below, the current values are shown as 'Date (YYMMDD): 00.00.00' and 'Time (hhmmss): 00:30:22'.
- Customer information:** Three text input fields for 'Location name', 'Function name', and 'Customer specific information'.
- Factory reset:** A 'Reset settings' label and a 'Start' button.

Figure 24: Device Settings > System

- **Power On Behavior:** Here you can configure the behavior when power is applied.
 - **User Interface:** Here you can set locks for the user.
 - **Date / Time:** The date and time can be taken from the PC used.
 - **Customer Information:** Individual customer information can be entered in the freely editable input fields.
- Factory Reboot:** The device can be reset to the factory settings.

Password

The screenshot shows the 'Password' configuration page with the following sections:

- Password protection:** A text input field for the 'Password'.
- Password protection level:** Radio buttons for 'Write protection active', 'Write and read protection active', and 'No password protection' (selected).

Figure 25: Device Settings > Password

- **Password Protection:** Here you can configure password protection settings.

! NOTICE

Do not transfer both settings at the same time!

Transferring both settings at the same time (with **[Submit]**) may cause an error. For more information on password handling, see [🔗 Device Parameter Object \[▶ 31\]](#).

Modbus

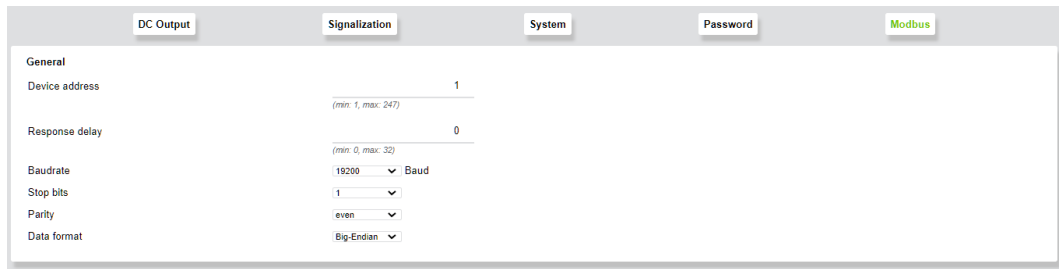


Figure 26: Device Settings > Modbus

- **General:** In this area, you can set specific parameters for the communication module.

See also

📄 Device Parameter Object [▶ 31]

9.1.6 Device Information

Here you can see the information on the lower-level device.

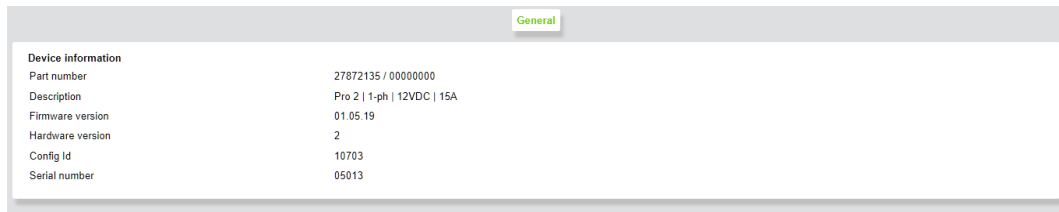


Figure 27: Device Information

9.1.7 Device Measurement

The **Measurement** page shows all the measured values and status information of the lower-level device.

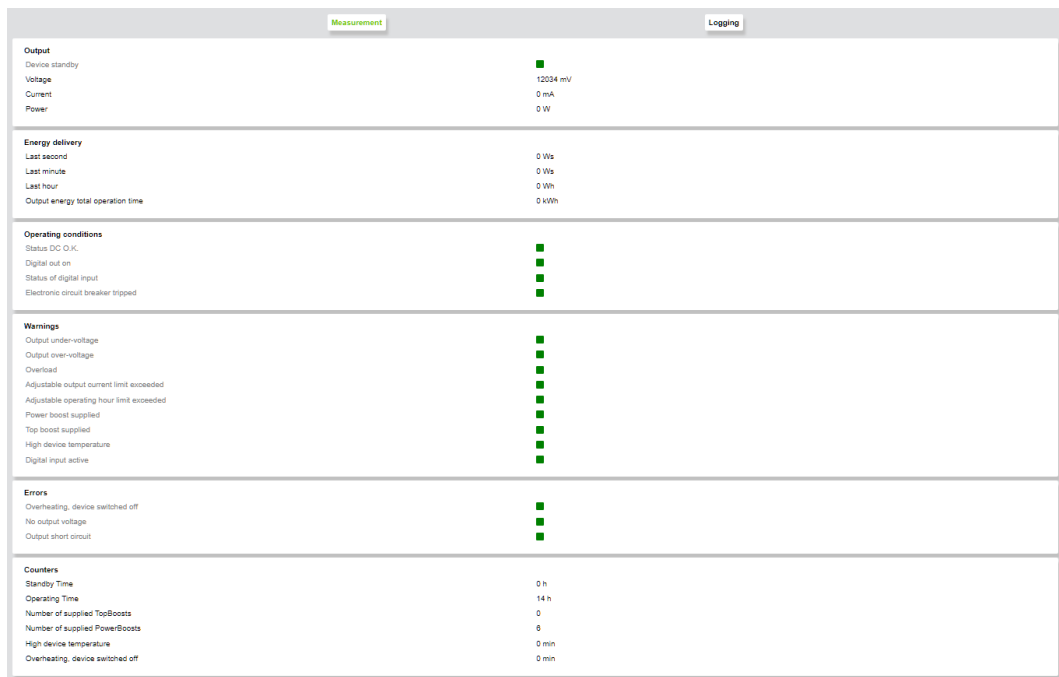


Figure 28: Measurement

- Green: function or state OK
- Red: function or state faulty/tripped

A history of the last error and warning messages can be viewed on the **Logging** page:

Measurement		Logging	
Error Logging			
Date	Time	Error Code	Warning Message
00.00.00	00.00.00		Output under-voltage
00.00.00	00.00.00		Output under-voltage High device temperature
00.00.00	00.00.00		Output under-voltage
00.00.00	00.00.00	No output	Output under-voltage
00.00.00	00.00.00		Output under-voltage
00.00.00	00.00.00		
00.00.00	00.03.40	short circuit	Output under-voltage Overload
00.00.00	00.03.40	short circuit	Output under-voltage Overload Power boost supplied
00.00.00	00.03.41	No output short circuit	Output under-voltage Overload Power boost supplied
00.00.00	00.03.51	No output short circuit	Output under-voltage Overload
00.00.00	00.03.55	short circuit	Output under-voltage Overload
00.00.00	00.03.55	short circuit	Output under-voltage
00.00.00	00.03.55		Output under-voltage
00.00.00	00.03.55		
00.00.00	00.03.05		Output under-voltage
00.00.00	00.03.05		Output under-voltage
00.00.00	00.03.05		Output under-voltage Overload Power boost supplied
00.00.00	00.03.05		Output under-voltage Overload Power boost supplied
00.00.00	00.03.05	short circuit	Output under-voltage Overload Power boost supplied

Figure 29: Device Measurement > Logging

9.1.8 Configuration of Communication with Broker

The communication between the communication module and a broker can be configured via the WBM (Web-Based-Management) under **Module Settings > MQTT** (see [Mod-ule Settings \[► 53\]](#)). Establishing the MQTT connection requires the broker to support the same protocol version as the communication module.

Establishing an Unencrypted Connection

1. In the **Broker Settings > IP Address** area, set the IP address of the broker.

Broker settings

IP-Address

192 . 168 . 1 . 200

Certificate Upload

Choose File

Figure 30: IP Address of the Broker

2. In the **Client Settings** area, the preconfigured settings can be adjusted to the use case:

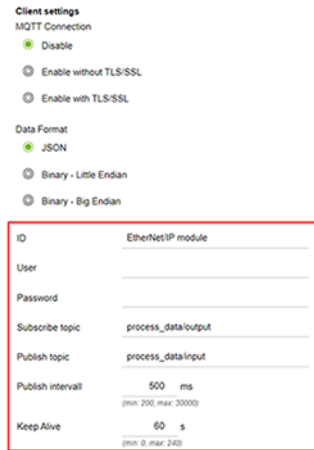


Figure 31: Application-Specific Settings

3. In the **Client Settings > MQTT Connection** area, select the **Enable without TLS/SSL** option to connect to the broker.

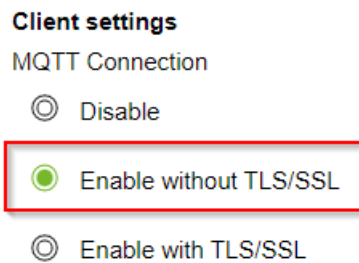


Figure 32: Enabling without TLS/SSL

⇒ The current status of the connection is shown under **MQTT Connection Status**.

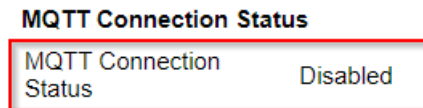


Figure 33: Connection Status

Establishing an Encrypted Connection:

1. In the **Broker Settings > IP Address** area, set the IP address of the broker.

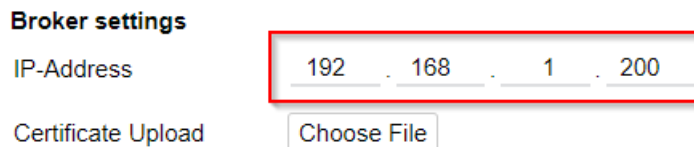


Figure 34: IP Address of the Broker

2. In the **Client Settings** area, the preconfigured settings can be adjusted to the use case:

Client settings

MQTT Connection

Disable

Enable without TLS/SSL

Enable with TLS/SSL

Data Format

JSON

Binary - Little Endian

Binary - Big Endian

ID

User

Password

Subscribe topic

Publish topic

Publish intervall
(min: 200, max: 30000)

Keep Alive
(min: 0, max: 240)

Figure 35: Application-Specific Settings

3. Create certificate (see [User Certificates \[▶ 67\]](#)).
4. Update the module date/time (see [Module Settings \[▶ 53\]](#)).
5. In the **Broker Settings > Certificate Upload** area, upload the CA file that has been created.

Broker settings

IP-Address

Certificate Upload

Figure 36: Selecting the Certificate File

6. In the **Client Settings > MQTT Connection** area, select **Enable with TLS/SSL** to connect to the broker.

Client settings

MQTT Connection

- Disable
- Enable without TLS/SSL
- Enable with TLS/SSL

Figure 37: Enabling with TLS/SSL

⇒ The current status of the connection is shown under **MQTT Connection Status**.


MQTT Connection Status

MQTT Connection Status

Figure 38: Connection Status

Decommissioning

10.1 Disposal and Recycling

	WEEE Mark Electrical and electronic equipment may not be disposed of with household waste. This also applies to products without this mark.
---	---

Electrical and electronic equipment contain materials and substances that can be harmful to the environment and health. Electrical and electronic equipment must be disposed of properly after use. Environmentally friendly disposal benefits health, protects the environment from harmful substances in electrical and electronic equipment and enables sustainable and efficient use of resources.

- Observe the national and local regulations for the disposal of electrical and electronic equipment, lithium-ion batteries, lead–acid batteries and packaging.
- Clear any data stored on electrical and electronic equipment.
- Remove lithium-ion batteries, lead–acid batteries or memory cards that are added to the electrical and electronic equipment.
- Wear appropriate personal protective equipment when removing the lithium-ion batteries/lead–acid batteries.
- Dispose of the removed lithium-ion batteries/lead–acid batteries according to your local waste regulations (e. g. collection boxes at the retail or local collection points).
- Have electrical and electronic equipment sent to a local collection point.
- Dispose of all types of packaging to ensure a high level of recovery, reuse and recycling.
- Transport packages from the B2B area can be taken back free of charge via a return system in accordance with the Packaging Act. Please contact our service provider Interseroh directly. The corresponding certificate can be found at: [🌐 corporate-certificates](#)
- Throughout Europe, Directives 2006/66/EC, 94/62/EC and 2012/19/EU (WEEE) apply. National directives and laws may differ.

Appendix

11.1 User Certificates

A certificate allows a secure connection for network communication and is used for authenticating the remote host. The lock icon in the browser indicates that this website has a valid, trusted certificate and that the connection is secure. We recommend replacing the self-signed certificates generated in the product with your own.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 192.168.1.17. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

[Learn more...](#)

Go Back (Recommended)

Advanced...

192.168.1.17 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

Error code: [MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT](#)

[View Certificate](#)

Go Back (Recommended) Accept the Risk and Continue

Figure 39: Browser warning message due to self-signed certificate

Certificates you create yourself must be signed by a certificate authority (the so-called root CA). The root certificate forms the shared trust anchor for all certificates subordinate to it and must be stored in the local trust store of the browser or client. The following sections describe an example of creating keys and certificates with the XCA key management software. This free software allows you to create certificates yourself. The certificates/keys are stored in a local database file. The database, which contains private keys among other things, is protected with a password.

11.1.1 Creating and Replacing Certificates

The following table lists the available cipher suites¹⁾:

Table 56: Available Cipher Suites

IANA No.	Cipher Suite
TLS1.3	
0x13, 0x01	TLS_AES_128_GCM_SHA256
0x13, 0x02	TLS_AES_256_GCM_SHA384
0x13, 0x04	TLS_AES_128_CCM_SHA256
0x13, 0x05	TLS_AES_128_CCM_8_SHA256
TLS1.2	
0xC0, 0xAC	TLS_ECDHE_ECDSA_WITH_AES_128_CCM
0xC0, 0xAE	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
0xC0, 0xAF	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8
0xC0, 0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
0xC0, 0x0A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
0xC0, 0x2B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
0xC0, 0x2C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
0xC0, 0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
0xC0, 0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

1) A standardized set of algorithms to ensure a secure network connection.

11.1.2 Creating a Template for Certificates

1. Open the XCA software and select the **New Database** submenu under the **File** menu.
2. Select a storage location and an appropriate name for the database.
3. Enter a password to protect the database.
 - ⇒ The newly created database opens.

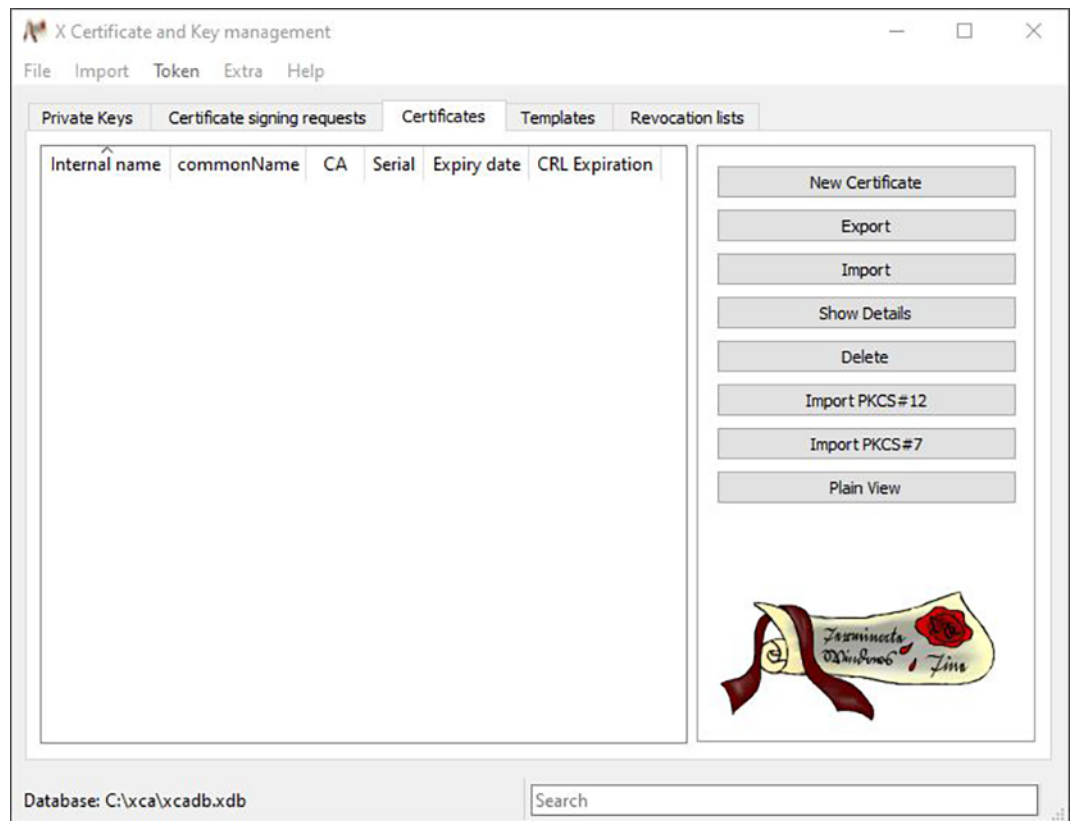


Figure 40: XCA Database

4. On the **Templates** tab, click the **[New Template]** button.
5. Select the “[Default] Blank Template” setting in the **Preset Template Values** dialog that opens.
6. Click **[OK]** to confirm the selection.
7. In the **Change XCA Template** dialog that opens, switch to the **Owner** tab.

Figure 41: Owner Tab

Input Field	Explanation
Internal name	The value in this field serves as an internal reference and should identify the certificate uniquely
countryName	Country code (e.g., DE for Germany)
stateOrProvinceName	State or province (e.g., NRW for North Rhine-Westphalia)
localityName	Place where certificate was issued
organizationName	Name of the organization that issued the certificate
organizationUnitName	Department identifier
commonName	A general identifier can be stored here
emailAddress	An email address can be stored here

8. Fill in the marked input fields in the upper section.
 - ⇒ The **commonName** field is left blank in the template and filled out later.
9. Click **[OK]** to confirm the entries.
 - ⇒ Once the template has been created, it is displayed in the window.

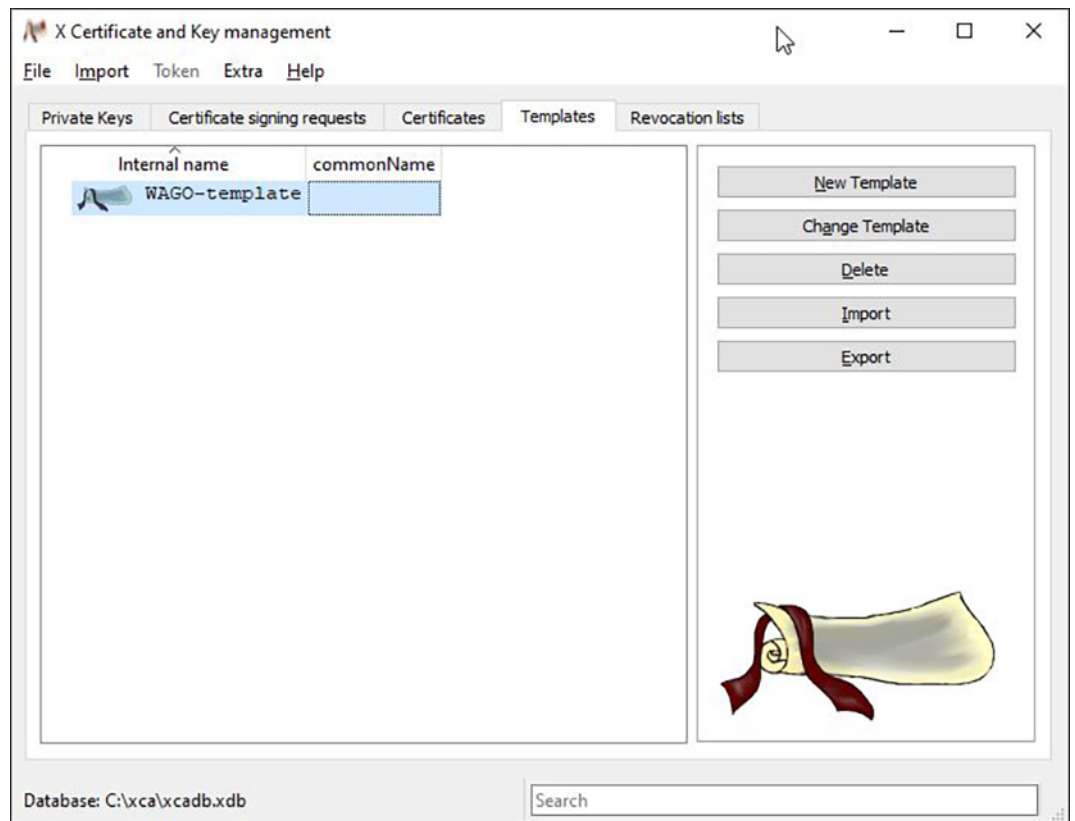


Figure 42: Creating a Template

11.1.3 Creating the Root CA Certificate

1. Switch to the **Certificates** tab to create the Root CA certificate. Click the **[New Certificate]** button.
 - ⇒ The following dialog appears.

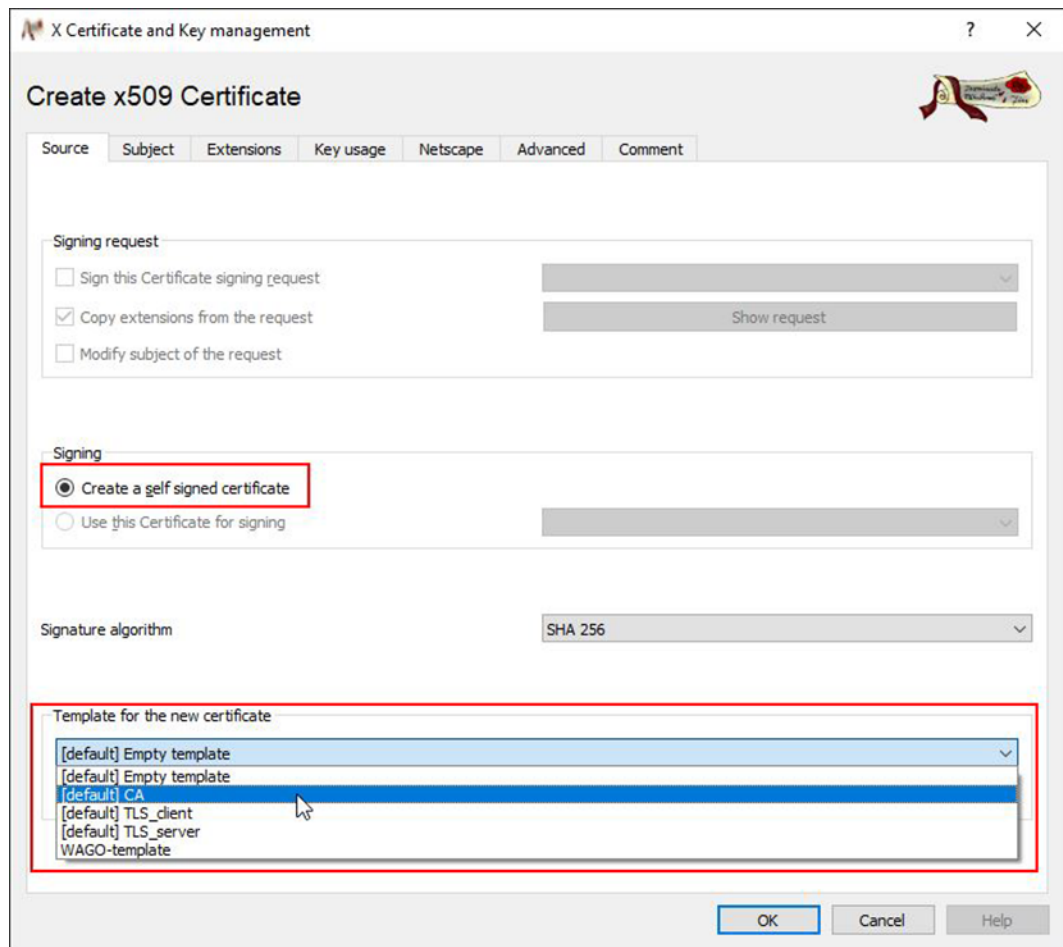


Figure 43: Creating a Certificate – Selecting a Template

2. Select your created template from the **Template for the New Certificate** selection field.
3. Click the **[Apply Subject]** button.
4. Select the **[Default] CA** template from the **Template for the New Certificate** selection field.
5. Click the **[Apply Extensions]** button.
6. Switch to the **Owner** tab.
 - ⇒ The following dialog appears.

X Certificate and Key management

Create x509 Certificate

Source Subject Extensions Key usage Netscape Advanced Comment

Internal Name

Distinguished name

countryName	DE	organizationalUnitName	BU IF
stateOrProvinceName	NRW	commonName	Root_CA
localityName	Minden	emailAddress	info@wago.com
organizationName	WAGO GmbH & Co. KG		

Type	Content
------	---------

Private key

Used keys too **Generate a new key**

OK Cancel Help

Figure 44: Creating a Certificate – Entering a Name

7. Enter an identifier in the **CommonName** input field (e.g., “Root_CA”).
8. Click the **[Create a New Key]** button.

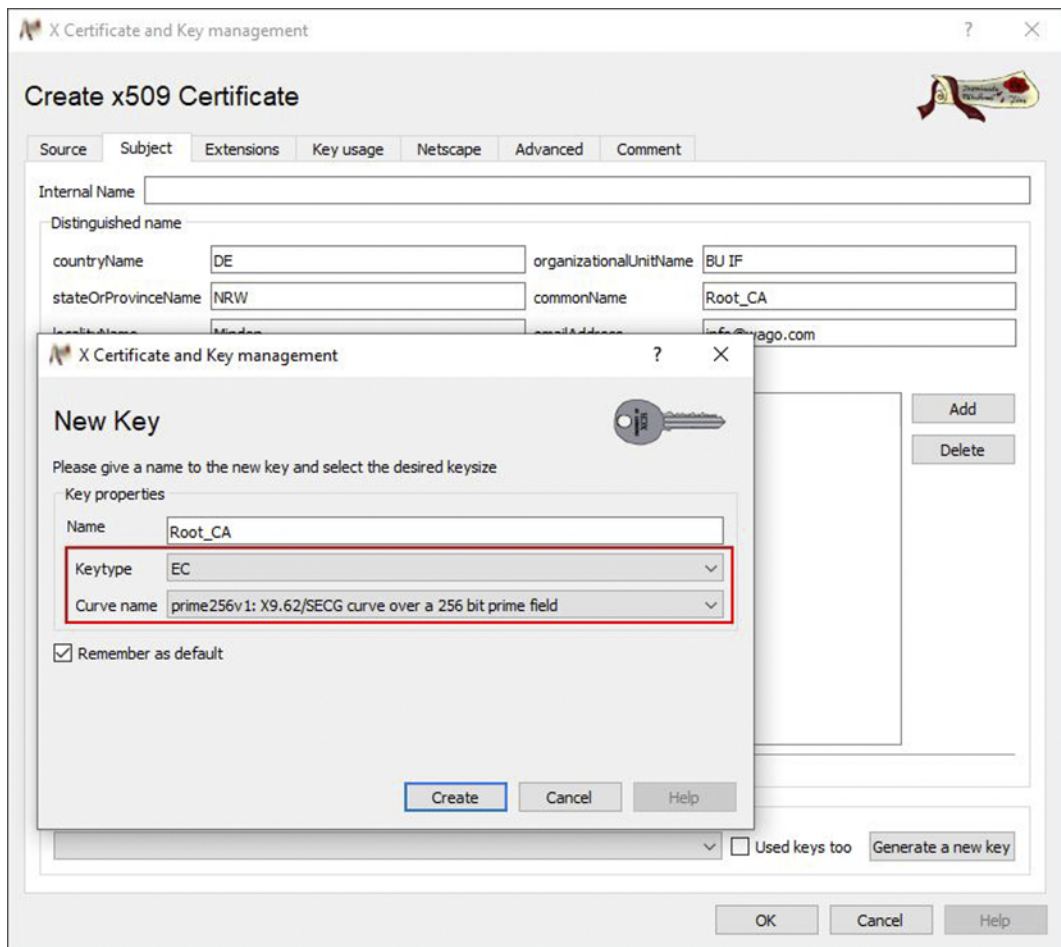


Figure 45: Creating a New Key

9. Set the key type to “EC” and select an EC curve for the root CA. The name is preset. The assignment depends on whether the key is generated for the root CA or for the module. The prime256r1 curve according to BSI TR 02102 2 (named prime256v1 in the XCA) is supported.

Note

No RSA keys are supported.

10. Click the **[Create]** button to create the key.
11. Click **[OK]** to exit the dialog after notification of successful key creation.
 - ⇒ The created certificate is displayed on the **Certificates** tab.

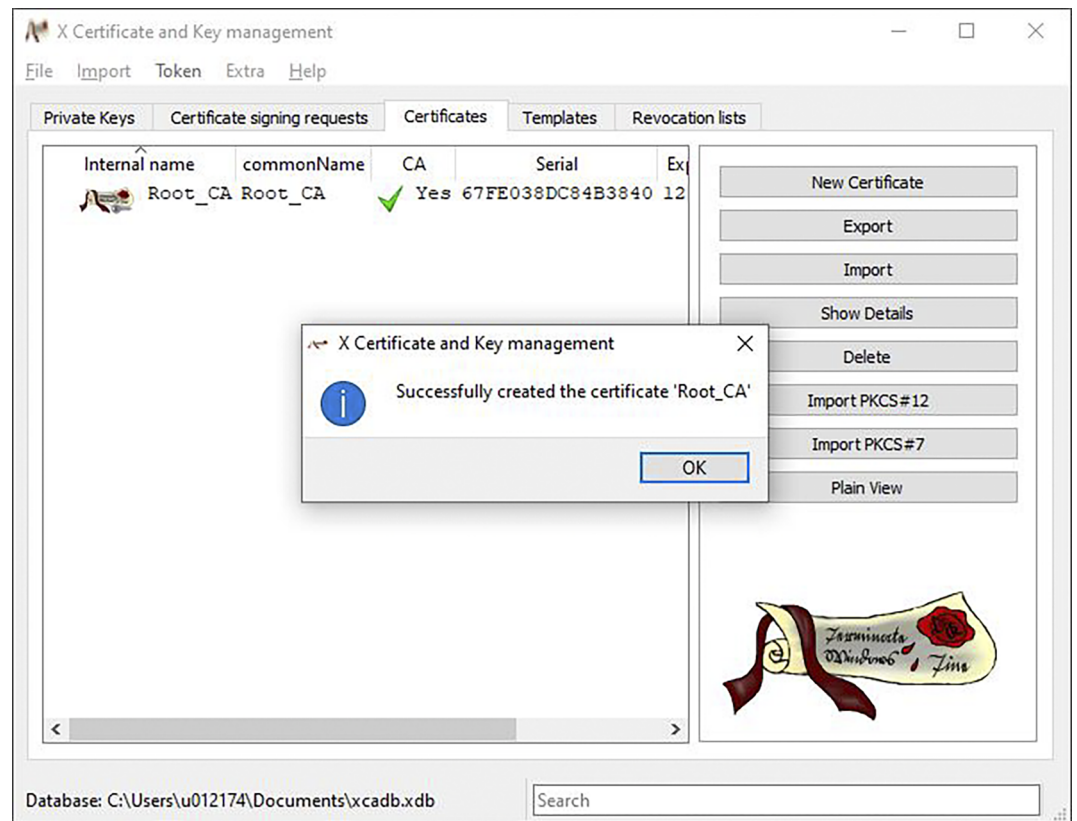


Figure 46: New Certificate Created

11.1.4 Creating the Device Certificate

1. Go to the **Certificates** tab to create the device certificate.
2. Click the **[New Certificate]** button.
 - ⇒ The following dialog appears.

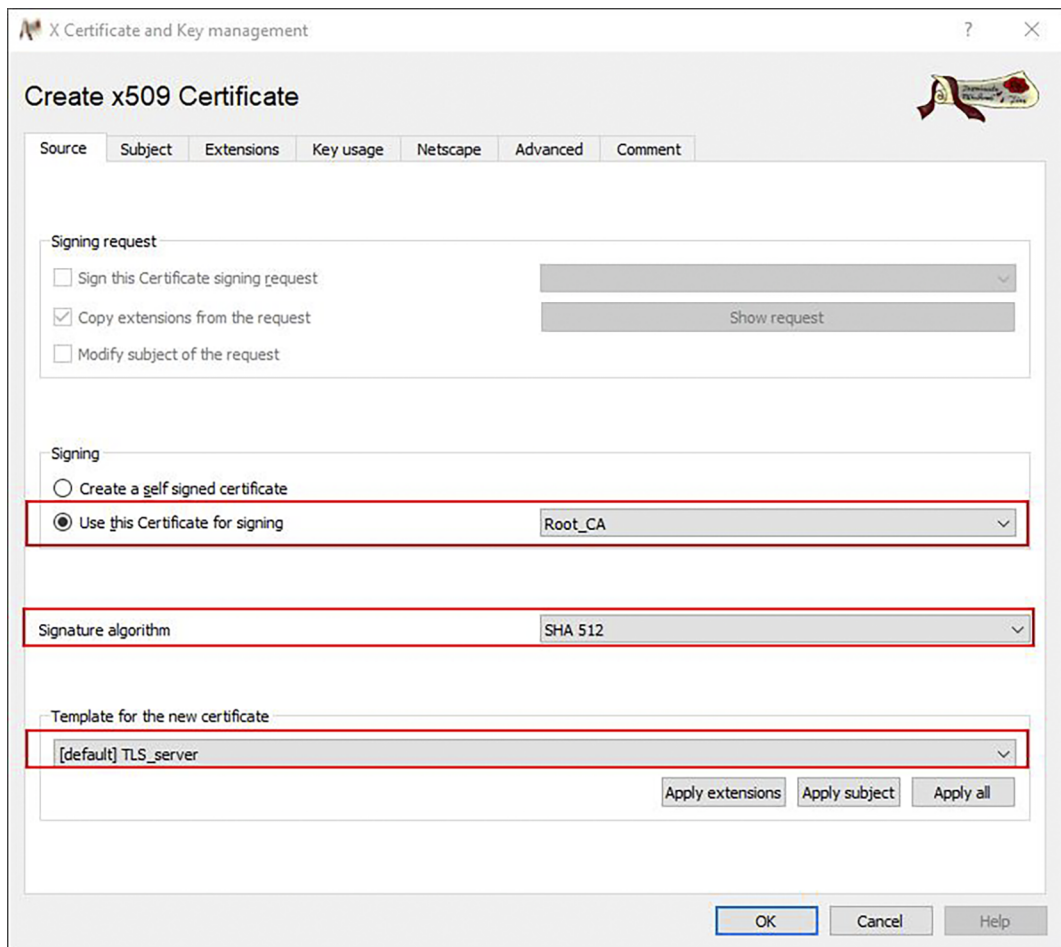


Figure 47: Creating a New Device Certificate

3. Check the **Use This Certificate for Signing** box and select the root CA certificate that has been created.
4. In the **Signature Algorithm** selection field, select the value “SHA 512” (see the BSI TR-02102 technical guidelines).
5. Select the template you created from the **Template for the New Certificate** selection field.
6. Click the **[Apply Subject]** button.
7. From the **Template for the New Certificate** selection field, select the “[Default] TLS_server” template.
8. Click the **[Apply Extensions]** button.
9. Switch to the **Owner** tab.
10. In the **CommonName** input field, enter the IP address of your server device. For WBM certificate creation, the IP address of the communication module is entered here. For MQTT certificate creation, the IP address of the broker is entered.
11. Click the **[Create a New Key]** button.

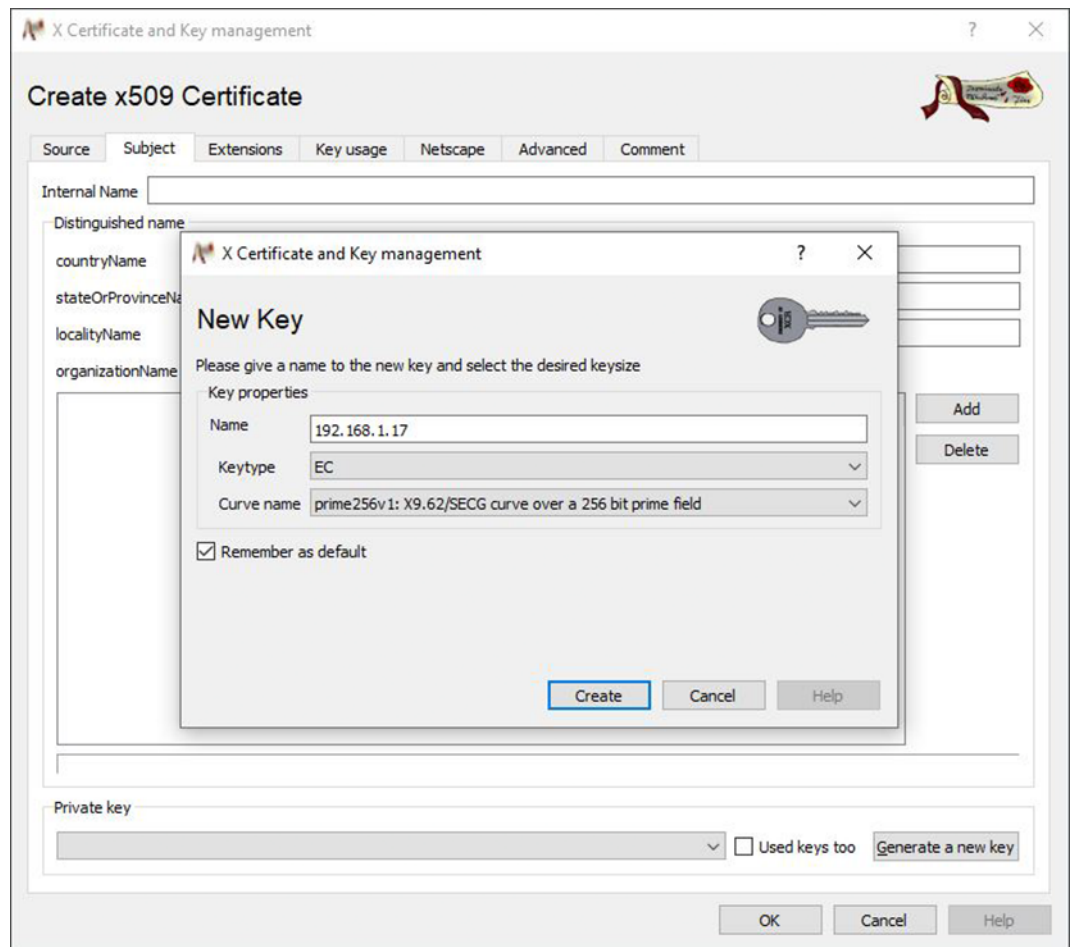


Figure 48: Creating a New Key

12. Change the key type to elliptic curve and select the prime256v1 curve.
13. Click the **[Create]** button to create the key.
14. Switch to the **Extensions** tab.

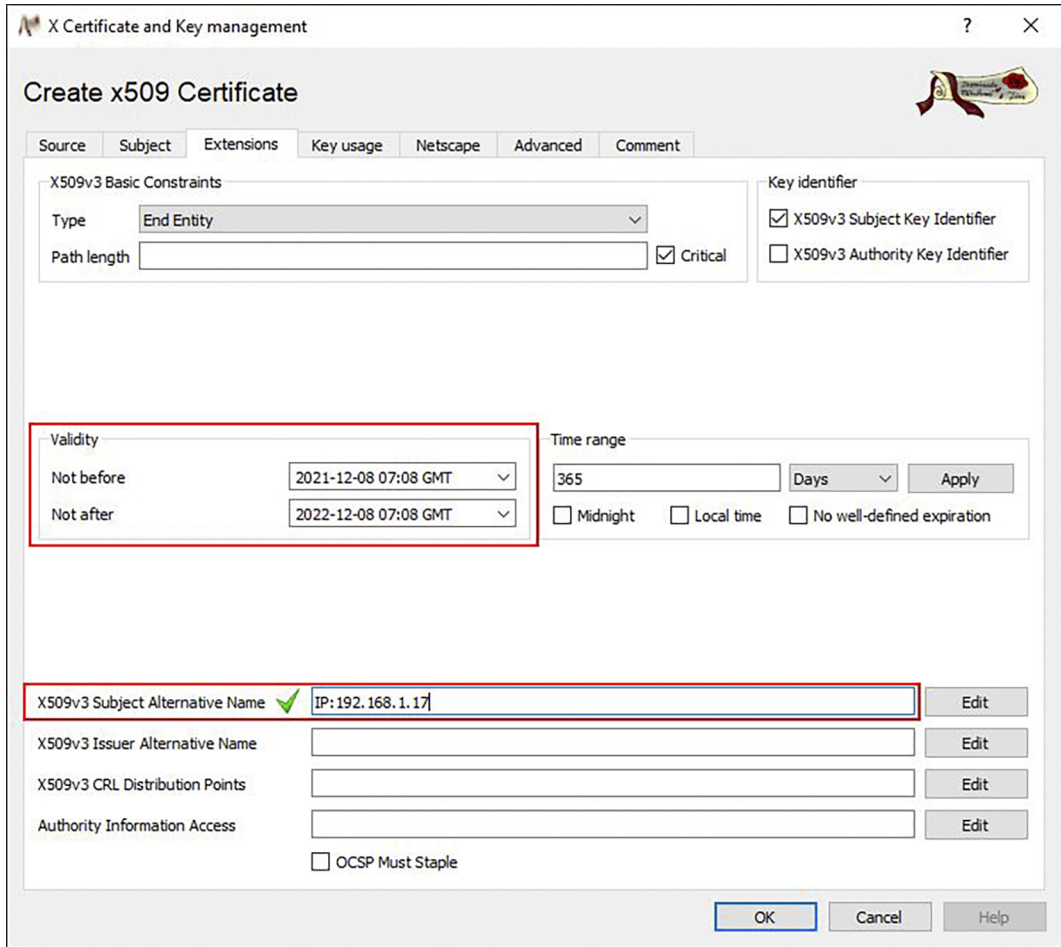


Figure 49: "Extensions" Tab

15. Set the validity of the device certificate. Please note the recommendations of the BSI TR-02102-2 technical guidelines.

16. Add the IP address and/or host name in the **X509v3 Subject Alternative Name** input field.

Note The value in the "X509v3 Subject Alternative Name" input field must be identical to server address!

Browsers use the IP address/host name to determine the identity. If the value entered in the **X509v3 Subject Alternative Name** input field differs from the value of the server's IP address, the certificate is identified as invalid!

17. Switch back to the **Key Management** tab to restrict the use of the certificates.

18. Enter the values marked in the figure.

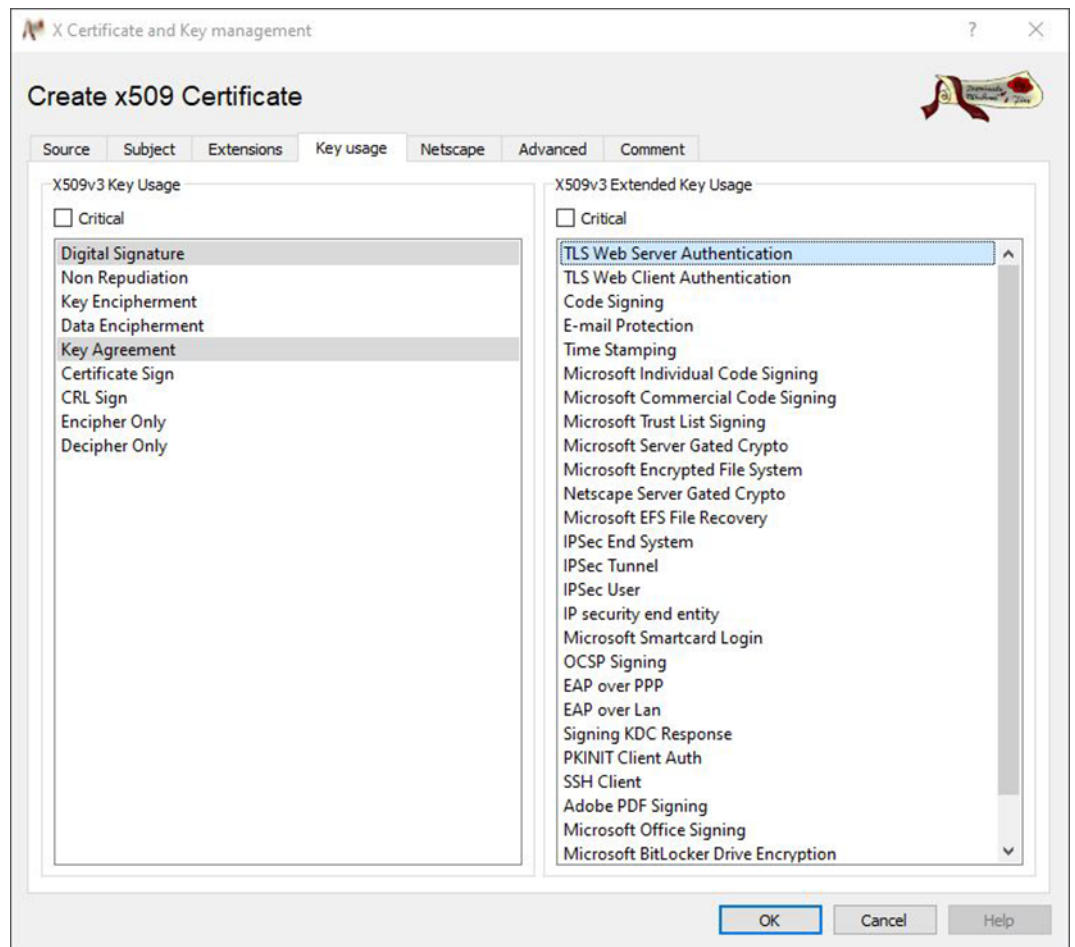


Figure 50: New Certificate Request, "Client" Key Use

19. Click **[OK]** to confirm the entries. The new certificate is shown below the root CA certificate on the **Certificates** tab.

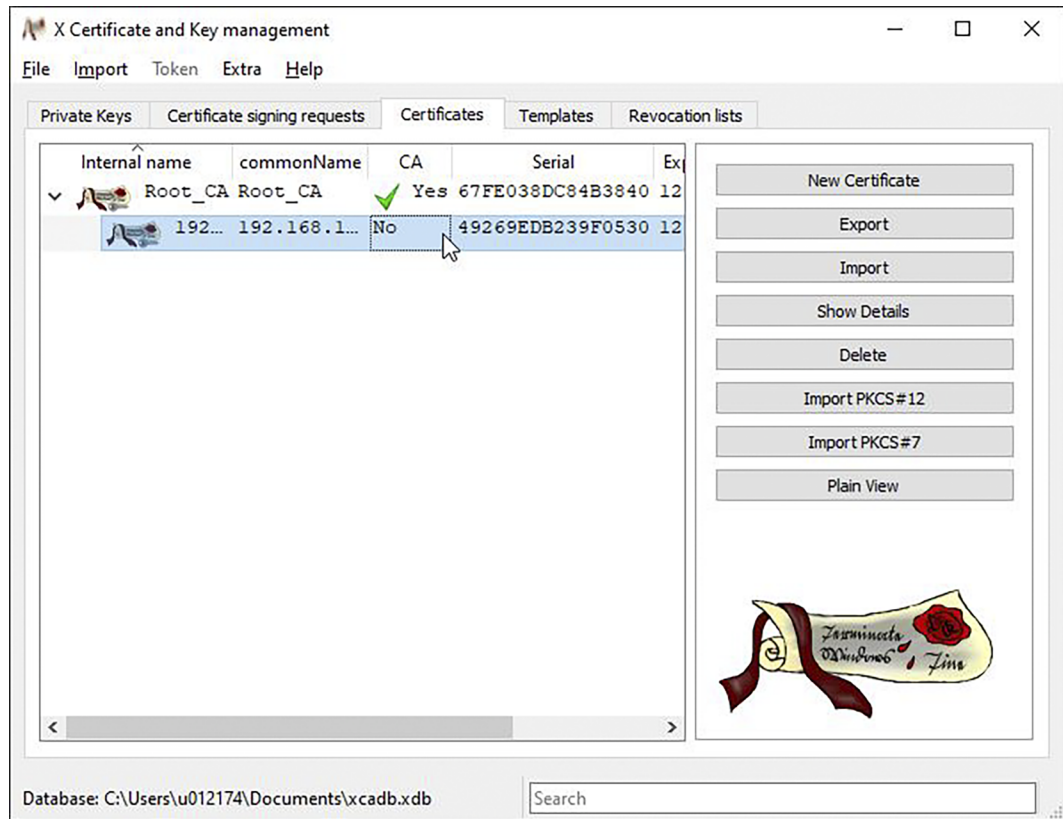


Figure 51: Device Certificate Created

11.1.5 Exporting WBM Certificates

1. In the main window, switch to the **Certificates** tab and expand the tree structure fully.
2. Select your root CA certificate and open the context menu by right-clicking.
3. Select **Export > File**.

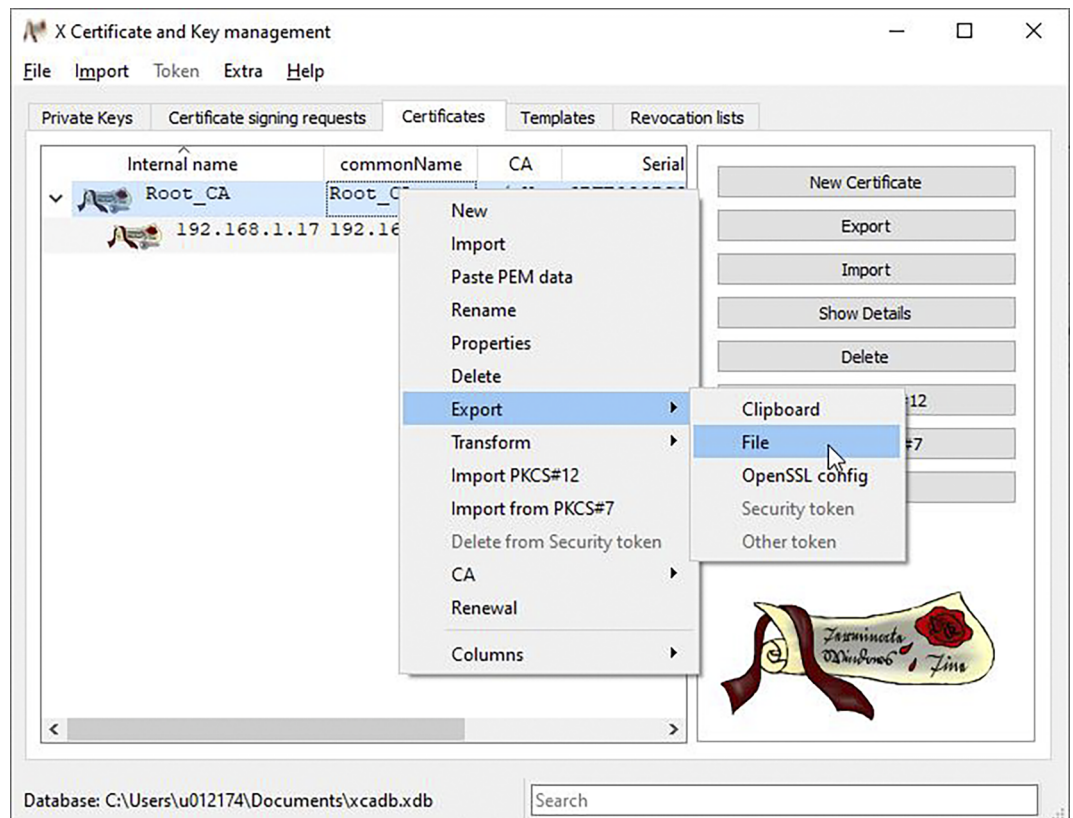


Figure 52: Exporting Root CA Certificate 1

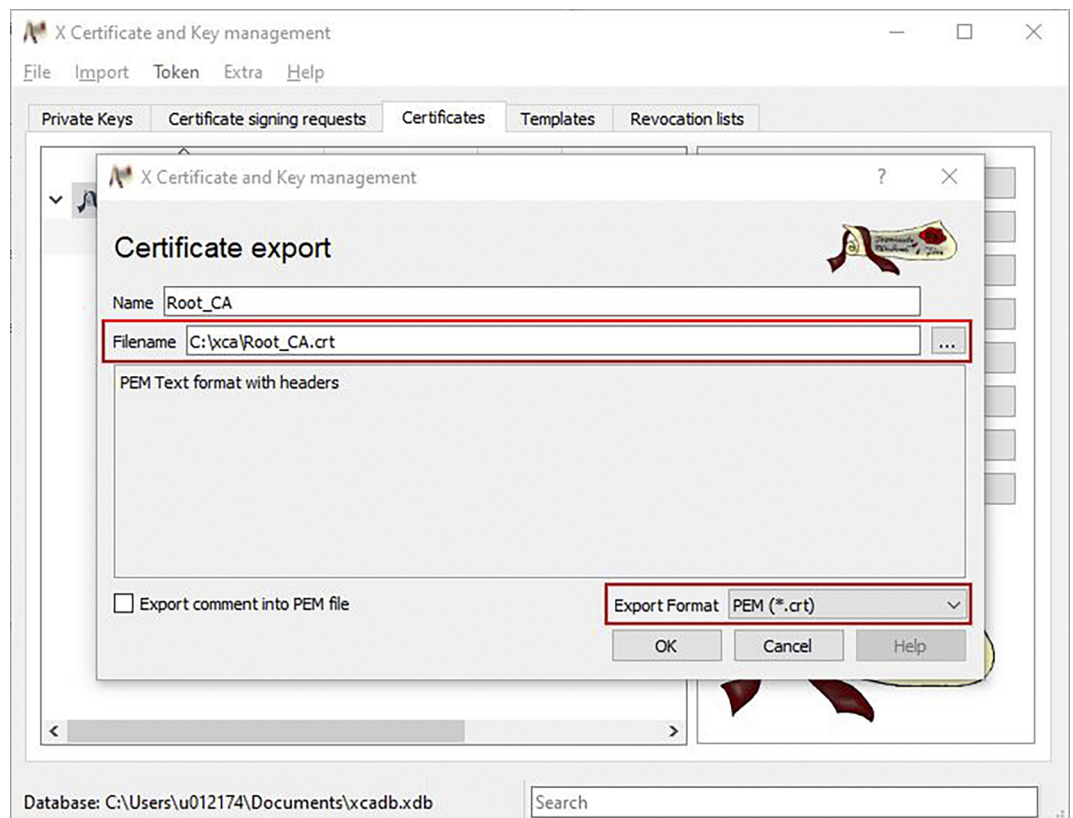


Figure 53: Exporting Root CA Certificate 2

4. Select the storage location by clicking the [...] button.
5. From the **Export Format** selection list, select the “PEM (*.crt)” entry.

6. Click **[OK]** to confirm.
7. Select your device certificate and right-click to open the context menu.
8. Select **Export > File**.

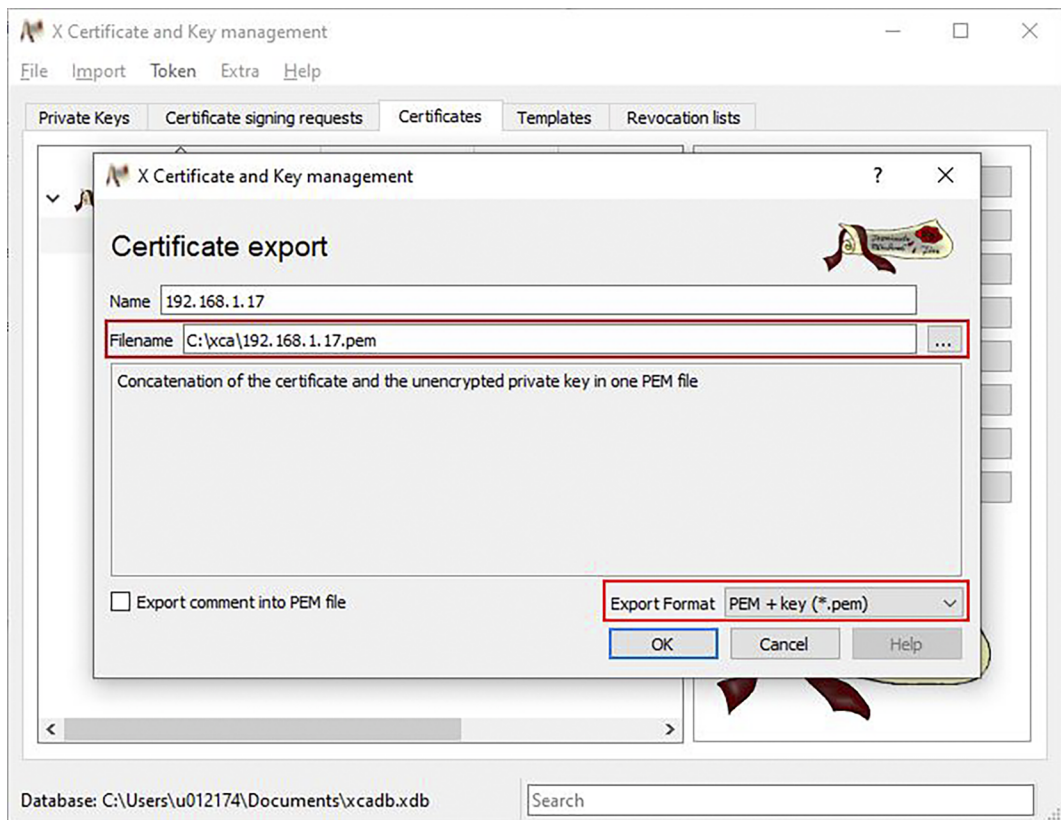


Figure 54: Exporting the Device Certificate

9. Select a storage location by clicking the **[...]** button.
10. From the **Export Format** selection list, select the “PEM with Key” entry.
11. Click **[OK]** to confirm.

11.1.6 Exporting MQTT Certificates

1. In the main window, switch to the **Certificates** tab and expand the tree structure fully.
2. Select your root CA certificate and right-click to open the context menu.
3. Select **Export > File**.

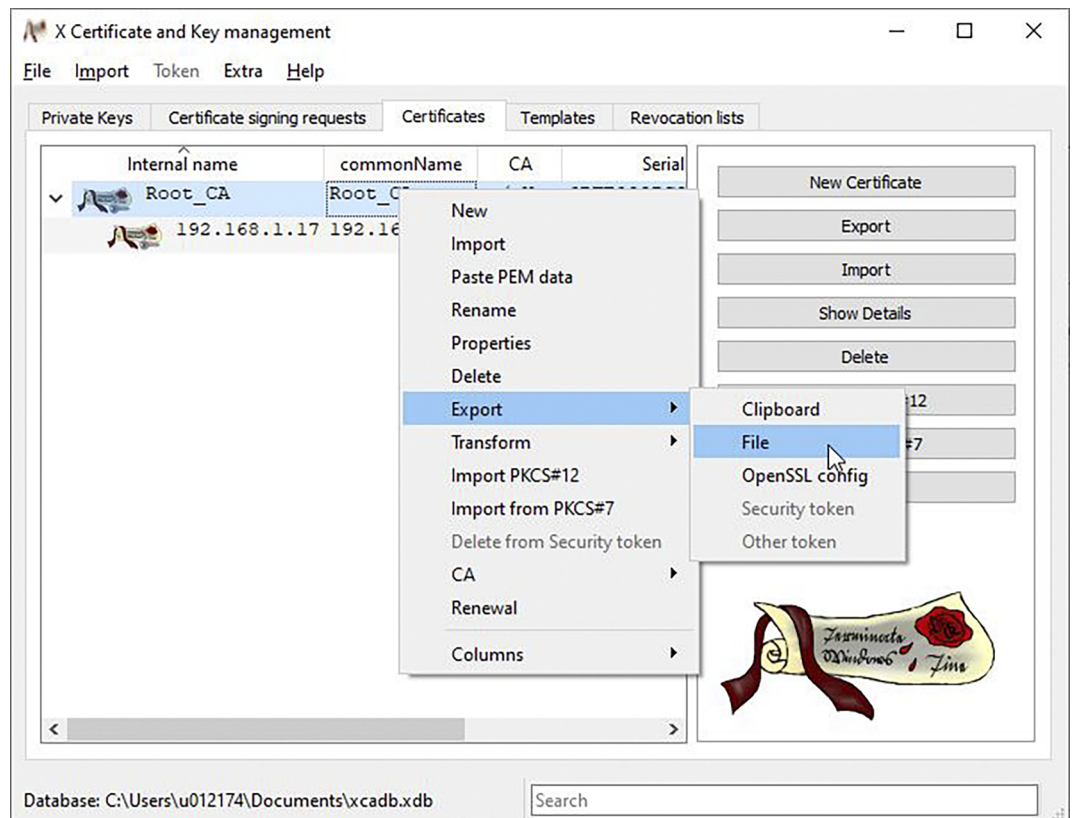


Figure 55: Exporting Root CA Certificate 1

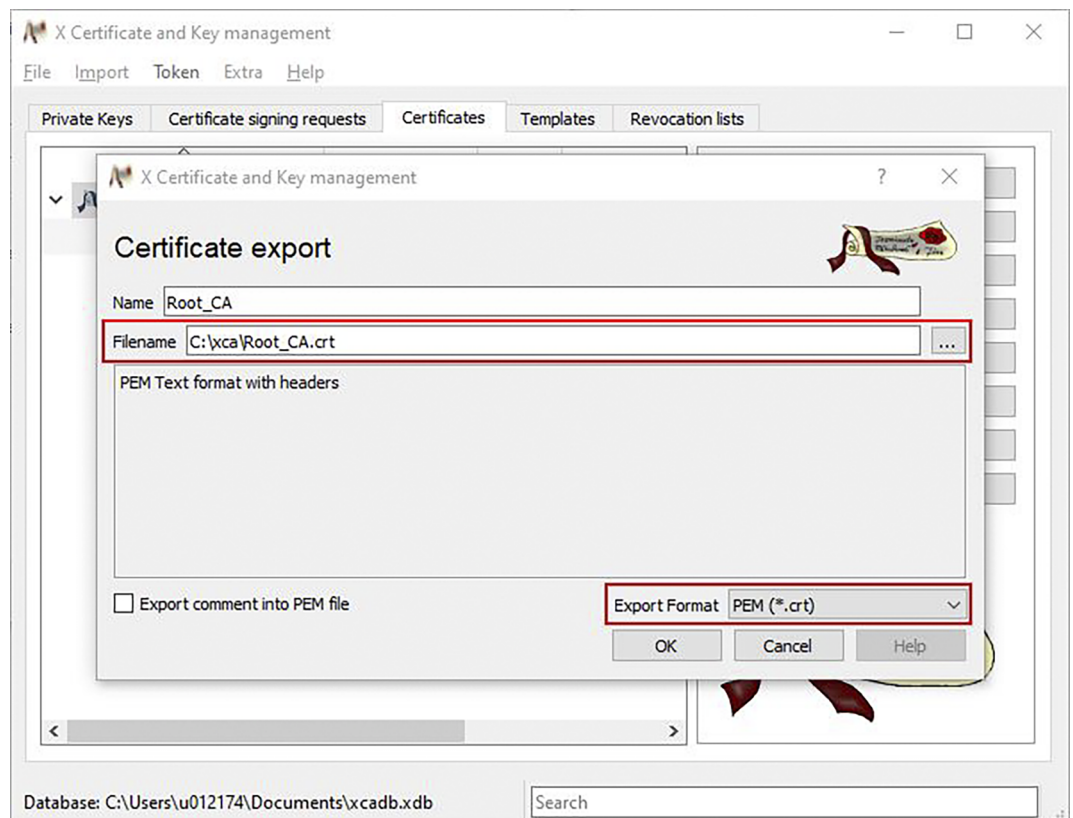


Figure 56: Exporting Root CA Certificate 2

4. Click the [...] button to select the storage location.
5. From the **Export Format** selection list, select the “PEM (*.crt)” item.

6. Click **[OK]** to confirm.
7. Select your device certificate and right-click to open the context menu.
8. Select **Export > File**.

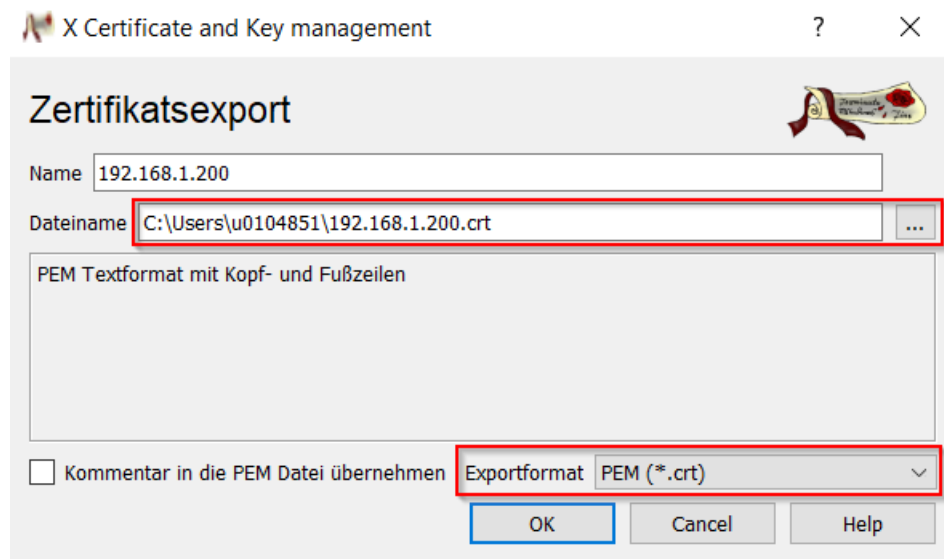


Figure 57: Exporting Broker Certificate

9. Select a storage location by clicking the [...] button.
10. In the **Export Format** selection list, select the “PEM without Key” item.
11. Click **[OK]** to confirm.
12. In the main window, switch to the **Private Key** tab.
13. Select your device certificate and right-click to open the context menu.
14. Select **Export > File**.

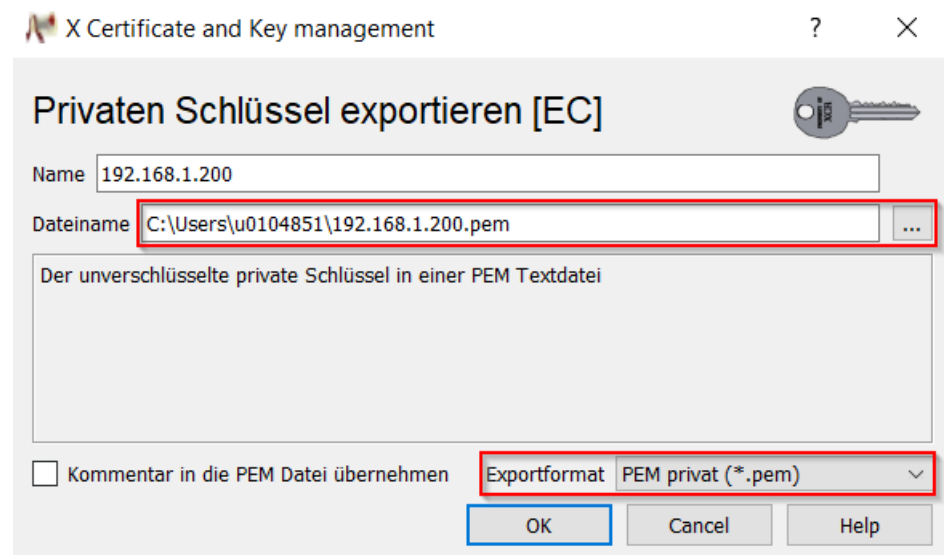


Figure 58: Exporting Broker Key

15. Click the [...] button to select a storage location.
16. From the **Export Format** selection list, select the “PEM private” item.
17. Click **[OK]** to confirm.

11.1.7 Installing WBM Certificates on the Client and Product

Note

New device certificate is necessary if IP address/host name changes!

If the IP address or host name has changed, the certificate must be recreated for the device with the correct IP address or host name (see [🔒 Creating the Device Certificate \[▶ 75\]](#)!)

1. Import your root CA certificate into the browser. The procedure depends on the browser used.
2. Transfer your device certificate to the product via the WBM. On the **Module Settings > Network** page, under **TLS Certificates**, click **[Choose File]**.

Figure 59: Importing the Device Certificate

3. Select the certificate you created and click **[Save Certificate]**.
 4. Reboot by clicking the **[Start]** button under “**Reboot**” on the **Module Settings > System** page.
- ⇒ As soon as a lock icon appears to the left or right (depending on the browser) of your Web address, the action has been successful, and your connection is secure from now on. Browsers often indicate how trusted a connection is in the address bar. For example, Firefox displays a lock icon if the certificate is signed by a trusted root CA.

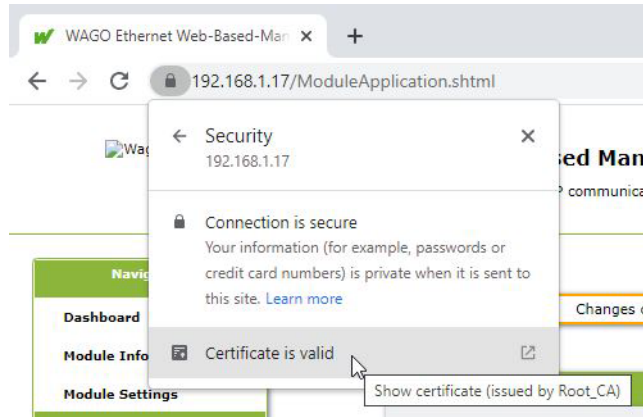


Figure 60: Importing the Device Certificate – Secure Connection

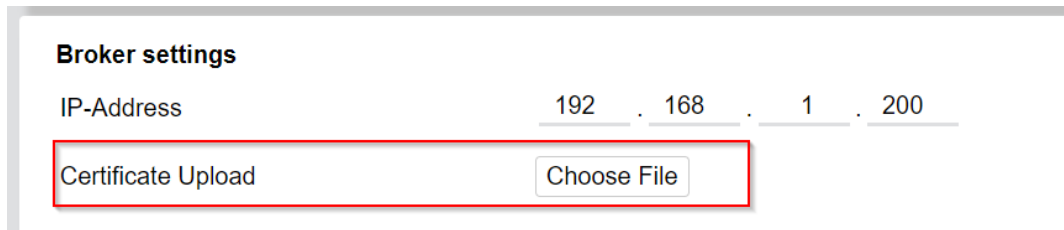
11.1.8 Installing MQTT Certificates on the Broker and Product

Note

New broker certificate is necessary if IP address/host name changes!

If the IP address or host name of the broker has changed, the certificate must be recreated with the correct IP address or host name (see [Creating the Device Certificate \[▶ 75\]](#))!

1. Transfer your root CA certificate to the product via the WBM. On the **Module Settings > MQTT** page, under **Certificate Upload**, click **[Choose File]**.

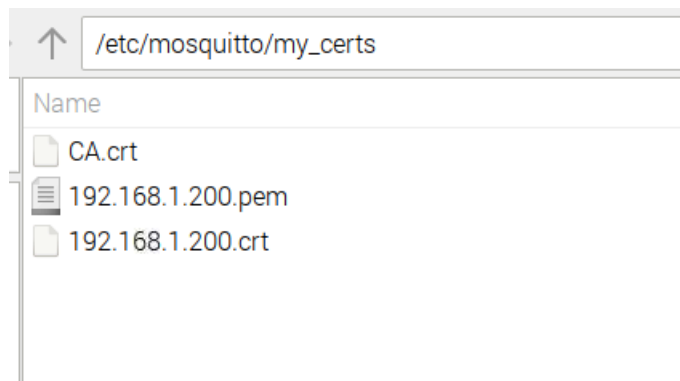


2. Import your root CA certificate and device certificate into the broker. The process depends on the browser used.

Note The import process depends on your browser!

The following steps apply to the Mosquitto broker.

3. Store the certificates in a specified folder.



4. Enter the names and paths of the certificates and the key in the mosquitto.conf file.

```

GNU nano 5.4 /etc/mosquitto/mosquitto.conf *
# Place your local configuration in /etc/mosquitto/conf.d/
#
# A full description of the configuration file is at
# /usr/share/doc/mosquitto/examples/mosquitto.conf.example

pid_file /run/mosquitto/mosquitto.pid

persistence true
persistence_location /var/lib/mosquitto/

log_dest file /var/log/mosquitto/mosquitto.log

include_dir /etc/mosquitto/conf.d

listener 1883
allow_anonymous true

listener 8883

certfile /etc/mosquitto/my_certs/192.168.1.200.crt
keyfile /etc/mosquitto/my_certs/192.168.1.200.pem
cafile /etc/mosquitto/my_certs/CA.crt

```

11.2 Accessories

The following accessories are available for the product:

Accessories – Marking

Table 57: Accessories – Marking

Description	Item Number
Marker Carrier	2789-1233
Marking System	2009-0110
WMB Multi Marking System	2009-0115
	2009-0115/0000-0002

Accessories – Other

Table 58: Accessories – Other

Description	Item Number
ETHERNET connector RJ-45; IP20; ETHERNET 10/100 Mbit/s; for field assembly	750-975
ETHERNET connector; RJ-45; Cat. 6A; straight; Code T568A; AWG 22	750-977/000-011
ETHERNET connector; RJ-45; Cat. 6A; straight; Code T568A; AWG 22; Strain relief	750-978/000-011
ETHERNET connector; RJ-45; Cat. 6A; angled; Code T568A; AWG 22; Strain relief	750-979/000-011

11.3 Protected Rights

- Adobe® and Acrobat® are registered trademarks of Adobe Systems Inc.
- Android™ is a trademark of Google LLC.
- Apple, the Apple logo, iPhone, iPad and iPod touch are registered trademarks of Apple Inc. registered in the USA and other countries. “App Store” is a service mark of Apple Inc.
- AS-Interface® is a registered trademark of the AS-International Association e.V.

- BACnet® is a registered trademark of the American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc. (ASHRAE).
- *Bluetooth*® is a registered trademark of Bluetooth SIG, Inc.
- CiA® and CANopen® are registered trademarks of CAN in AUTOMATION – International Users and Manufacturers Group e.V.
- CODESYS is a registered trademark of CODESYS Development GmbH.
- DALI is a registered trademark of the Digital Illumination Interface Alliance (DiiA).
- EtherCAT® is a registered trademark and patented technology licensed by Beckhoff Automation GmbH, Germany.
- ETHERNET/IP™ is a registered trademark of the Open DeviceNet Vendor Association, Inc (ODVA).
- EnOcean® is a registered trademark of EnOcean GmbH.
- Google Play™ is a registered trademark of Google Inc.
- IO-Link is a registered trademark of PROFIBUS Nutzerorganisation e.V.
- KNX® is a registered trademark of the KNX Association cvba.
- Linux® is a registered trademark of Linus Torvalds.
- LON® is a registered trademark of the Echelon Corporation.
- Modbus® is a registered trademark of Schneider Electric, licensed for Modbus Organization, Inc.
- OPC UA is a registered trademark of the OPC Foundation.
- PROFIBUS® is a registered trademark of the PROFIBUS Nutzerorganisation e.V. (PNO).
- PROFINET® is a registered trademark of the PROFIBUS Nutzerorganisation e.V. (PNO).
- QR Code is a registered trademark of DENSO WAVE INCORPORATED.
- Subversion® is a trademark of the Apache Software Foundation.
- Windows® is a registered trademark of Microsoft Corporation.

List of Tables

Table 1	Revision index structure.....	14
Table 2	Operating Status Indication.....	16
Table 3	Technical Data – Product.....	16
Table 4	Technical Data – Power Loss	17
Table 5	Technical Data – Communication	17
Table 6	Technical Data – Environmental Conditions	17
Table 7	Approvals	18
Table 8	Mechanical and Climatic Environmental Conditions	19
Table 9	EMV – Immunity to Interference	19
Table 10	EMC – Emission of Interference	19
Table 11	Overview of CIP Common Classes.....	21
Table 12	Overview of WAGO-Specific Classes	21
Table 13	Explanation of the Table Headings in the Object Descriptions	21
Table 14	Data Types Used	21
Table 15	Identity Object – Instance 0	22
Table 16	Identity Object – Instance 1	22
Table 17	Common Services.....	24
Table 18	Assembly Object – Instance 101, Attribute ID 3	25
Table 19	Assembly Object – Instance 102	25
Table 20	Common Services.....	26
Table 21	TCP/IP Interface Object – Instance 0	26
Table 22	TCP/IP Interface Object – Instance 1	27
Table 23	Common Services.....	28
Table 24	Ethernet Link Object – Instance 0.....	28
Table 25	Ethernet Link Object – Instance 1 (Port 1).....	29
Table 26	Ethernet Link Object – Instance 2 (Port 2).....	30
Table 27	Common Services.....	31
Table 28	General Device Parameters – Device Identification	31
Table 29	General Device Parameters – “Password Level” Parameter	32
Table 30	General Device Parameters – Modbus.....	33
Table 31	Parameters – DC Output	34
Table 32	Parameters – Electronic Circuit Breaker Mode.....	34
Table 33	Parameter – Signaling – Digital Input	34
Table 34	Parameter – Signaling – Digital Output.....	34
Table 35	Parameters – System	35
Table 36	Common Services.....	35

Table 37	Internal Module Parameters – Cross-Device Information for Identification.....	36
Table 38	Internal Module Parameters – General ETHERNET Settings	36
Table 39	Internal Module Parameters – Switch Settings for Channel 1	36
Table 40	Internal Module Parameters – Switch Settings for Channel 2	37
Table 41	Internal Module Parameters – Date	37
Table 42	Internal Module Parameters – Time.....	38
Table 43	Common Services.....	38
Table 44	Events and Measured Values – Process Input Data	38
Table 45	Events and Measured Values – Status Messages	39
Table 46	Events and Measured Values – Warnings.....	39
Table 47	Events and Measured Values – Errors	39
Table 48	Events and Measured Values – Power/Energy	40
Table 49	Common Services.....	40
Table 50	MQTT Connection Status	41
Table 51	Reading Out Process Data in JSON Format	41
Table 52	Writing Process Data in JSON Format	42
Table 53	Reading Out Process Data in Binary Format.....	43
Table 54	Writing Process Data in Binary Format.....	43
Table 55	Using the Reset Button	51
Table 56	Available Cipher Suites.....	68
Table 57	Accessories – Marking.....	87
Table 58	Accessories – Other.....	87

List of Figures

Figure 1	View	12
Figure 2	Product-Specific Information	14
Figure 3	RJ45 Interface, X5/X6	15
Figure 4	Visual Status Indicator	16
Figure 5	Raspberry Pi as MQTT Broker	44
Figure 6	WAGO PFC 200 as MQTT Broker	44
Figure 7	Mounting	46
Figure 8	Removal	47
Figure 9	Module Settings > Network	49
Figure 10	Module Settings > System	50
Figure 11	Login with Read/Write Protection	52
Figure 12	Login with Read Protection	52
Figure 13	Menu Page	53
Figure 14	Module Settings > System	53
Figure 15	Module Settings > MQTT	55
Figure 16	Module Settings > EtherNet/IP	55
Figure 17	Module Settings > Network	56
Figure 18	Module Settings > Parameter Management	57
Figure 19	Module Settings > Switch settings	57
Figure 20	Module Information > General	58
Figure 21	Module Information > Customer	58
Figure 22	Device Settings > DC Output	59
Figure 23	Device Settings > Signalization	60
Figure 24	Device Settings > System	61
Figure 25	Device Settings > Password	61
Figure 26	Device Settings > Modbus	62
Figure 27	Device Information	62
Figure 28	Measurement	62
Figure 29	Device Measurement > Logging	63
Figure 30	IP Address of the Broker	63
Figure 31	Application-Specific Settings	64
Figure 32	Enabling without TLS/SSL	64
Figure 33	Connection Status	64
Figure 34	IP Address of the Broker	64
Figure 35	Application-Specific Settings	65
Figure 36	Selecting the Certificate File	65

Figure 37	Enabling with TLS/SSL	65
Figure 38	Connection Status	65
Figure 39	Browser warning message due to self-signed certificate.....	67
Figure 40	XCA Database	69
Figure 41	Owner Tab	70
Figure 42	Creating a Template	71
Figure 43	Creating a Certificate – Selecting a Template	72
Figure 44	Creating a Certificate – Entering a Name	73
Figure 45	Creating a New Key	74
Figure 46	New Certificate Created.....	75
Figure 47	Creating a New Device Certificate.....	76
Figure 48	Creating a New Key	77
Figure 49	“Extensions” Tab.....	78
Figure 50	New Certificate Request, “Client” Key Use	79
Figure 51	Device Certificate Created	80
Figure 52	Exporting Root CA Certificate 1	81
Figure 53	Exporting Root CA Certificate 2	81
Figure 54	Exporting the Device Certificate	82
Figure 55	Exporting Root CA Certificate 1	83
Figure 56	Exporting Root CA Certificate 2	83
Figure 57	Exporting Broker Certificate	84
Figure 58	Exporting Broker Key	84
Figure 59	Importing the Device Certificate.....	85
Figure 60	Importing the Device Certificate – Secure Connection	86

WAGO GmbH & Co. KG

Postfach 2880 · D - 32385 Minden
Hansastraße 27 · D - 32423 Minden

✉ info@wago.com
🌐 www.wago.com

Headquarters	+49 571/887 – 0
Sales	+49 (0) 571/887 – 44 222
Order Service	+49 (0) 571/887 – 44 333
Fax	+49 571/887 – 844169